UiO : Det juridiske fakultet

Hvordan skape tillitsfull bruk av teknologi?

De ulike implikasjoner av teknologibruk for kriminalitetsforebygging

Oda Kibsgaard-Petersen

Masteravhandling i kriminologi ved Institutt for kriminologi

og rettssosiologi ved Juridisk fakultet

Våren 2023

Hvordan skape tillitsfull bruk av teknologi?

De ulike implikasjoner av teknologibruk for kriminalitetsforebygging

Sammendrag

Tittel: Hvordan skape tillitsfull bruk av teknologi? De ulike implikasjoner av teknologibruk for kriminalitetsforebygging

Skrevet av: Oda Kibsgaard-Petersen

Veileder: Helene O. I. Gundhus

Levert ved: Juridisk fakultet – Institutt for kriminologi og rettssosiologi, våren 2023

Vi ser i dag store endringer i hvordan politiet arbeider forebyggende. I økende grad benyttes digital teknologi med formål om å forhindre kriminalitet. Også kunstig intelligens og maskinlæring implementeres i slike verktøy. I andre land har vi sett hvordan bruken av prediktiv teknologi kan føre med seg en rekke ulike samfunnsmessige implikasjoner. Diskriminering, skjevheter i data og overvåkningspraksiser har ført til kritikk mot politimyndigheter. I forskningslitteratur finnes det dermed gjerne en utbredt kritisk holdning til slik teknologibruk. I Norge er denne typen teknologi i stor grad fremdeles på et utviklingsstadium. Det er derfor interessant å undersøke hvordan en slik overførbarhet vil kunne se ut i det norske samfunnet, der utgangspunktet for styring er åpenhet, inkludering og gjennomsiktighet. **Formålet** med denne avhandlingen er å undersøke hvilket mulighetsrom som finnes i Norge for å skape en tillitsfull bruk av teknologi innenfor kriminalitetsforebygging. Samtidig har det vært ønskelig å se nærmere på hva personer som innehar beslutningsprosesser på dette fagfeltet mener skal til for å drive frem en tillitsfull forebygging. For å gjøre dette har **fremgangsmåten** for studien bestått av individuelle intervjuer med syv informanter som arbeider innenfor det aktuelle fagfeltet. Metoden har dermed vært kvalitativ intervjuanalyse. Relevante aktørers holdninger, synspunkt og narrativ har dannet avhandlingens grunnlag. Studiens funn presenteres hovedsakelig i lys av relevant **tidligere forskning** på feltet, samt et **teoretisk rammeverk** som kan knyttes til ulike disipliner innenfor kriminologi.

I selve **analysen** belyses det hvilke holdninger informantene har til forebyggende teknologi. Informantene fremmer en teknologioptimisme, og vektlegger den samfunnsnytten forebyggende teknologi kan inneha. De trekker linjer til land og aktører de mener at norske myndigheter bør se til i forbindelse med teknologiimplementering, samt land de mener er dårlige eksempler. Informantene beskriver videre de ulike utfordringer som finnes ved

forebyggende teknologi. De trekker frem mangelfullt datagrunnlag, ulike skjevheter som kommer til uttrykk i teknologi, mangelen på transparens og tillit, samt teknologiens overvåkningspotensial. Mot slutten av analysen rettes fokus mot hvordan det på best mulig måte kan tilrettelegges for tillitsfull bruk av forebyggende teknologi. Godt datagrunnlag, kunnskap og kompetanse om teknologi, ansvarsfordeling og tverrfaglighet, samt transparens er hovedtrekkene i informantenes synspunkter. I etterkant av analysen vil det være et **diskusjonskapittel**, som skal belyse avhandlingens funn i en bredere sosial kontekst. I diskusjonen stilles det spørsmål som: Vil fremtidens forebyggende praksis kunne komme i konflikt med de prinsipper Norge står for? Hvordan påvirkes politirollen av den økende teknologibruken? Hvilken type forebygging fremmer informantene? Hvilket overvåkningspotensial har teknologien? Og hvordan definerer vi egentlig samfunnstillit?

Nøkkelord: kriminalitetsforebygging, teknologi, kunstig intelligens, maskinlæring, tillit, pre-crime, overvåkning, sosial kontroll, stordata.

FORORD

Denne masteravhandlingen markerer slutten på et fem år langt kapittel som kriminologistudent ved Universitetet i Oslo. Det siste året har vært en spennende og utfordrende prosess. Jeg er nå stolt og glad for å kunne sette punktum for studenttilværelsen med denne oppgaven, som det har blitt lagt ned utallige timer med arbeid for å skrive. Jeg valgte et tema som jeg kunne svært lite om fra før av, men som jeg syntes virket veldig interessant. Dette har ført til at skriveprosessen har vært krevende, men også veldig lærerik. I tillegg har jeg skrevet en oppgave som har gjort seg mer samfunnsrelevant i tiden jeg har holdt på med den.

Det er mange som fortjener en stor takk i forbindelse med studien min. Først og fremst ønsker jeg å takke alle informantene som stilte opp. Takk for at dere tok dere tid til meg, viste engasjement og ga meg mange nyttige og gode innspill til prosjektet.

Tusen takk til veilederen min, Helene O. I. Gundhus. Du har hjulpet meg massevis gjennom det siste året. Jeg har satt så utrolig stor pris på alle kloke råd du har gitt meg i oppgaveskrivingen. Du har hele tiden vært tilgjengelig for meg når jeg har trengt det og strukket deg langt for å kunne gi meg tilbakemeldinger. Jeg setter også pris på tålmodigheten din gjennom alle utkastene jeg har levert. Du har samtidig latt meg delta på konferanser og workshops som har hjulpet meg til å finne inspirasjon til det jeg har skrevet om. Du har virkelig vært den beste veilederen jeg kunne ønske meg!

Jeg har også lyst å takke venner, familie og medstudenter for all hjelp og heiarop når jeg har trengt det. Jeg vil rette en spesiell takk til en nydelig mamma som har støttet meg gjennom hele prosessen, en fantastisk pappa som har hjulpet meg å korrekturlese, og ikke minst verdens beste kjæreste som har hjulpet meg å komme gjennom det siste året. Du har støttet, trøstet og lest gjennom oppgaven sammen med meg utallige ganger. Jeg setter så uendelig stor pris på deg.

Oda

Ålesund, mai 2023

Innholdsfortegnelse

In a jigsaw puzzle certain pieces are more important than others. For a piece of a jigsaw puzzle to contribute in a positive manner it has to be used with caution. If new pieces, which are blown out of proportion, are added, or if they are mistakenly perceived as more important than they actually are, or even worse do not belong to that particular jigsaw puzzle at all, then they might do more harm than help (Aas, Gundhus, & Lomell, 2009, s. 234).

1 Introduksjon

Det har skjedd store forandringer innen kriminalitetsforebygging det siste tiåret. Vi kan for eksempel se hvordan ulike typer teknologi tar større og større plass, både nasjonalt og globalt, og i økende grad blir den digitalisert. I dag er størsteparten av verden teknologisk avhengig. Det har igjen hatt påvirkning i arbeidet til politimyndigheter (Fyfe, Gundhus, & Rønn, 2018, s. 62). Bruken av teknologi bidrar til å endre hvordan politiet skal sikre sosial kontroll, håndtere lovbrudd og forebygge kriminalitet. Vi ser samtidig hvordan sikkerhet stadig flyter inn i kriminalitetskontrollen (Kaufman, 2018). Troen på at teknologi er en bærer av sikkerhet er en økende diskurs i samfunnet (Fyfe, Gundhus, & Rønn, 2018, s. 11). Det senmoderne samfunnet har dermed utvidet det som inngår i kriminalitetskontrollen til også å inkludere teknologi.

Året 2023 har vært preget av den kunstige intelligensens inntog. Med kunstig intelligens siktes det til dataprogrammers evne til å gjennomføre menneskelignende og kognitive funksjoner som å forstå, lære og reagere på egne omgivelser (Klepper, et al., 2021, s. 21). Gjennom fremskritt innen moderne teknologi er ikke bruken av kunstig intelligens lengre en fjern fremtid i science fiction. Ifølge flertallet av KI-eksperter er det 50 % sjanse for at vi i 2062 har skapt maskiner som er like intelligente som oss selv (Chan, 2021, s. 41). Vi kan allerede se tegn til en slik utvikling, der kunstig intelligens i høyeste grad preger dagens samfunnsdebatt. Hovedgrunnen til dette er utviklingen og implementeringen av nettsiden ChatGPT. Kunstig intelligens har imidlertid i lengre tid omgitt oss i et relativt stort omfang. Både telefonene våre, datamaskinene våre, bilene vi bruker og dataspillene vi spiller benytter en eller annen form for kunstig intelligens. Likevel har den allmenne oppmerksomheten i mindre grad vært rettet mot det som inngår i å skape slik teknologi. Dette kan tyde på at kunstig intelligens på mange måter har holdt seg usynlig, men vi ser nå et skifte hvor den blir mer synlig. Gjennom ChatGPT har teknologien begynt å ta valg for oss, gjøre vanskelige oppgaver for oss og kan etterligne våre rasjonelle tankesett. Når slik avansert kunstig intelligens plutselig har fått innpass i hverdagen vår, tydeliggjør dette potensialet teknologien innehar. KI har dermed inntatt dagsorden, både i mediebildet, innen teknologiutvikling og i forskningslitteraturen. For eksempel ga NTNU-forskeren Inga Strümke i månedsskiftet april – mai 2023, ut boken «Maskiner som tenker: Algoritmenes hemmeligheter og veien til kunstig intelligens». Den ble etter få dager utsolgt og ble påfølgende uke den boken som solgte aller mest i Norge (Norli, 2023). Dette illustrerer den voksende interessen for KI-feltet i samfunnet.

Samtidig slutter politiet i økende grad opp om kunstig intelligens som beslutningsverktøy for å forebygge kriminalitet og uorden. Teknologi er derfor tydelig med på å endre politiets samfunnsmandat og praksis.[1] Ambisjonene til kunstig intelligens er å skulle gjøre menneskelige beslutninger smartere, mer effektive og mer rasjonelle. Dette anses som positivt ettersom verden preges av stadig mer kompleks og omfangsrik informasjon, som er i rask endring (Chan, 2021, ss. 41-42). Ulike verktøy for prediktive analyser implementeres i dag i politiarbeid på tvers av ulike land. Slike analyser er avhengige av å identifisere ulike mønstre som kan gi kunnskap om fremtidig kriminalitet (Kaufman, Egbert, & Leese, 2018, s. 674), og kunstig intelligens brukes gjerne til å analysere data.

Fyfe, Gundhus og Rønn (2018, s. 13) reiser spørsmål om de mindre synlige implikasjonene av slik teknologi. Janet Chan (2021, s. 41) mener at fremtiden til kunstig intelligens vil avhenge av hvordan samfunnet selv ser på kunstig intelligens og dens relevans og nytteverdi. Forestillingene vi selv har om teknologibruk, vil derfor kunne være viktige i en slik diskusjon. Chan (2021, s. 4) viser samtidig til en utbredt diskusjon preget av uenigheter om hvorvidt vi skal se på kunstig intelligens som en velsignelse eller en forbannelse. Et viktig spørsmål er dermed hvordan fremtiden til kunstig intelligens vil kunne se ut i politiarbeid. Dette finnes det ikke noe klart svar på i verken litteratur eller i offentlige publikasjoner (Chan, 2021, s. 41).

Jeg mener på bakgrunn av dette at det vil være interessant å undersøke hvordan digital teknologi påvirker kriminalitetsforebyggingen i det norske samfunnet. Jeg ønsker å se nærmere på hvordan vi kan sikre en åpen debatt om demokratisk bruk av forebyggende teknologi, når teknologien i utgangspunktet er et spesialisert kompetanseområde. Jeg ønsker å se nærmere på hvordan forebyggende teknologi vil påvirke den tilliten som norske myndigheter innehar i dag. Dette gjør det også viktig å studere teknologien nærmere, da kunnskap om et fenomen er nødvendig for å forstå fenomenets rekkevidde. Kunstig intelligens vil være en sentral del av en slik diskusjon. Den teknologiske fremtiden er ifølge forskningslitteraturen usikker. Avhandlingens utgangspunkt er dermed å undersøke hvilke diskurser norsk offentlighet trekker veksler på for å best mulig tilpasse seg en slik utvikling.

[1] Dette er en del av det prosjektet «Algoritmisk styring og politikulturer i endring: perspektiver fra Norge, India, Brasil, Russland, Sør-Afrika og Nederland» ønsker å belyse. Prosjektet skal undersøke hvordan politiets bruk av kunstig intelligens, digital teknologi og private sikkerhets-/teknologi-/konsulentselskaper kan bidra til å endre politiets samfunnsmandat og praksis

1.1 Problemstilling og forskningsspørsmål

Hensikten med avhandlingen er å undersøke forebyggende teknologis implikasjoner, ulike holdninger og erfaringer til slik teknologi, samt hvorvidt det er mulig å skape tillitsfull bruk av den i kriminalitetsforebygging. Et viktig spørsmål er samtidig hvilken type forebygging som fremmes av teknologibruk. Et annet sentralt spørsmål er hvilke lovbrudd slike verktøy skal kunne være med å forebygge og hvilke tilsiktede og utilsiktede implikasjoner disse verktøyene har. Jeg mener det er interessant å undersøke hvordan teknologi påvirker det norske samfunnet der utgangspunktet for styring er åpenhet, inkludering og gjennomsiktighet. Hvorvidt forebyggende teknologi kan påvirke den eksisterende legitimiteten og tilliten norsk politi har, er også viktig å se nærmere på. Med utgangspunkt i avhandlingens introduksjon, har jeg valgt følgende problemstilling:

Hvordan kan vi skape en tillitsfull bruk av forebyggende teknologi for å forebygge fremtidig kriminalitet?

Med tillitsfull bruk sikter jeg til en bruk som gjenspeiler verdiene som preger det norske samfunnet i dag. En slik posisjon tar utgangspunkt i legitime og forutsigbare, rettferdige og upartiske institusjoner (Egge, Strype, & Thomassen, 2012, s. 11). Teknologi som innebefatter kunstig intelligens og maskinlæring er lite tematisert i det fremvoksende feltet digital kriminologi. Utgangspunktet til digital kriminologi er krysningen mellom kritisk, kulturell og sosioteknisk teori. Den digitale kriminologien favner de forskjellige epokene av teknologiske innovasjoner, samt de ulike tolkningene av teknologi (Powell, Stratton, & Cameron, 2018, s. 7). Innenfor digital kriminologi vises det til viktigheten av å studere den gjensidige påvirkningen mellom samfunn og teknologi (Powell, Stratton, & Cameron, 2018, s. 5). Denne avhandlingen har ambisjoner om å være et bidrag til det digitale kriminologifeltet. Som vist til innledningsvis, vil det også være et tema som er aktuelt og samfunnsrelevant.

1.2 Avhandlingens videre gang

Avhandlingen har totalt syv kapitler. Sett bort fra denne introduksjonen vil neste kapittel gi en beskrivelse av avhandlingens bakgrunn, gjennom tidligere forskningsbidrag. Her vil det som angår forebyggingsbegrepet, teknologi og implikasjoner av teknologi være sentralt. I dette kapittelet vil det også gis en definisjonsavklaring av kunstig intelligens, maskinlæring og øvrige tekniske begrep som vil være relevant for avhandlingens analyse.

I kapittel 3 presenteres avhandlingens teoretiske rammeverk. Her vil jeg trekke frem tre overordnede perspektiver som anvendes i analysen for å tolke informantenes synspunkter, narrativ og holdninger. Perspektivene omhandler overvåkning, sikkerhet og pre-kriminalitet. Samlet vil et slikt teorigrunnlag kunne gi et tydelig bilde av dagens kriminalitetsforebygging.
I kapittel 4 vil jeg ta for meg metodedelen av avhandlingen. Her vil de ulike metodiske avveiningene gjøres rede for. Dette inneholder valg av kvalitative verktøy, metodiske valg gjort før, underveis og i etterkant av arbeidet. Også etiske refleksjoner i forbindelse med prosjektet inngår her.
Kapittel 5 er analysekapittelet. Analysen består av fem deler: «hvilken teknologi snakker vi om?», «fremtidsrettede syn på teknologi», «hvem skal vi se til?», «utfordringer ved forebyggende teknologi» og «hvordan tilrettelegge for tillitsfull teknologi?».
Kapittel 6 og 7 vil inneholde avhandlingens diskusjonsdel, oppsummering og avslutning. Der vil hovedtrekkene fra analysen løftes frem og diskuteres.
Til slutt vil jeg gi en kort oppsummering av avhandlingen og noen avsluttende betraktninger.

2 Bakgrunn og tidligere forskning

Dette kapittelet presenterer bakgrunnen for avhandlingens relevans. Utvalgt tidligere forskning på det aktuelle feltet vil også trekkes frem. Det vil dermed ikke være en fullstendig gjennomgang av all forskning på det forebyggende teknologiske fagfeltet. Kapittelet er delt inn i fire deler. Først vil jeg forklare hva som ligger i forebyggingsbegrepet og i politiets forebyggingsmandat. Jeg vil så beskrive teknologiens vei inn i det forebyggende feltet. Videre gis en definisjonsavklaring av relevante begreper i teknologien; herunder kunstig intelligens, maskinlæring, stordata og algoritmer. Disse begrepene vil gjennomgående brukes i avhandlingen. Til slutt vil jeg ta for meg tidligere forskning på ulike implikasjoner av forebyggende teknologi innen kriminalitetsfeltet.

2.1 Politiets forebyggingsmandat

Av problemstillingens ordlyd, vil forebyggingsbegrepet inneha en sentral plass i avhandlingen. Derfor vil det være hensiktsmessig å gjøre rede for hva som ligger i politiets forebyggingsmandat. I politiloven (1995, § 1) står det skrevet følgende: «Politiet skal gjennom forebyggende, håndhevende og hjelpende virksomhet være et ledd i samfunnets samlede innsats for å fremme og befeste borgernes rettssikkerhet, trygghet og alminnelige velferd for øvrig». Gjennom politiloven ser vi tydelig hvordan kriminalitetsforebygging er en sentral del av politiets arbeidsoppgaver. Selv om det finnes ulike forståelser av forebygging, defineres gjerne politiets kriminalitetsforebyggende arbeid som de innrettelser politiet gjør for å unngå at kriminalitet oppstår, fremfor å måtte reparere i ettertid. Dette vil si at det er proaktivt og planlagt politiarbeid, i stedet for reaktivt politiarbeid som reagerer på kriminalitet som allerede har skjedd (Gundhus, 2014, ss. 178-179).

Hva som inngår i politiets forebygging, har vært i endring opp gjennom historien. Derfor har også de ulike forståelsene av hvordan politiet skal utføre forebyggingsmandatet vært det. Dette har ført til diskusjoner rundt hvilken målsetting, grad av ansvar og organisering som har vært i endring (Gundhus, 2014, s. 179). Den tradisjonelle forståelsen har i hovedtrekk omhandlet rettshåndhevelse og avskrekking. Også ideen om at det er situasjoner som muliggjør og skaper lovbrudd er en sentral tilnærming (Gundhus, 2014, s. 179). Dette har vært utgangspunktet for den situasjonelle kriminalitetsforebyggingen. Her defineres visse situasjoner som problematiske og vurderer hvordan en best og mest hensiktsmessig kan iverksette tiltak opp

mot dette. På siden av dette snakker man også om den sosiale kriminalitetsforebyggingen, som ser på både hvordan inkludering og ekskludering fremmer og hemmer kriminalitet, samt hvordan individuelle risikofaktorer forsterker kriminalitetskarrierer (Gundhus, 2014, ss. 184-185). Vi kan på bakgrunn av dette se at forebygging har vært på politiets agenda i svært ulik form.

Kriminalitetsforebygging som begrep har dermed blitt brukt på ulike måter for å tilnærme seg kriminalitetsproblemet. På ene siden har det vært beskrivende for ulike praksiser eller handlinger; altså har det vært knyttet opp mot ulike måter å redusere lovbrudd på. På andre siden har det blitt anvendt for å snakke om ulike måloppnåelser eller utfall av kriminalitetsreduksjon. Eksempel på dette er «lavere kriminalitetsrater i et lokalsamfunn» eller «mangelen på nye lovbrudd fra en gjerningsperson». Det er også svært ulike instanser som holder på med kriminalitetsforebygging (Byrne & Marx, 2011, s. 18). I Norge er samarbeid mellom politi og kommune sentralt for å forebygge kriminalitet og skape trygghet i lokalsamfunnet. Gundhus (2014, ss. 178-179) beskriver samtidig hvordan politiet har en dobbeltrolle i det forebyggende arbeidet; i første omgang skal politiet fremme forebygging og trygghet i samfunnet. I tillegg til dette, skal de også ha en nøkkelrolle i strafferettssystemets kriminalitetsforebygging. Gundhus tolker dermed forebyggingsbegrepet som «elastisk» i sin tilnærming.

2.2 Den digitale teknologiens vei inn i forebygging

Rollen som digital teknologi spiller i moderne politiarbeid, har ført til store endringer i kriminalitetskontrollen og i kriminalitetsforebygging (Byrne & Marx, 2011, s. 18). Teknologiske fremskritt har opp gjennom årene hatt en tydelig innflytelse på hvordan vi tenker om kriminalitet og innsatsen som gjøres for å forhindre den (Byrne & Marx, 2011, s. 21). En digital infrastruktur har lenge blitt beskrevet som noe som kan muliggjøre en effektiv politipraksis (Niculescu-Dincă, 2021, s. 76). Europol (2022) viser samtidig til at teknologi har stor innvirkning på kriminalitetens natur. På ene siden er det kriminelle som raskt integrerer og benytter ny teknologi. På andre siden skaper ny teknologi muligheter for rettshåndhevelse og for å møte nye trusler om kriminalitet. Teknologisk innovasjon kan eksempelvis bidra til at rettshåndhevende myndigheter får tilgang til egnede verktøy for å bekjempe kriminalitet. Et tredje perspektiv er hvordan teknologisk kontroll også skaper ulikhet, slik kritisk forskning på «overvåkningssamfunnet» har adressert (Lyon, 2007).

Byrne og Marx (2011, s. 18) gjør et skille mellom «myke» og «harde» teknologiske innovasjoner. Informasjonsbasert teknologi vil tilhøre de myke teknologiene, imens materialbasert teknologi vil defineres som hard teknologi. Begge former knyttes til en omveltning i hvordan politiet driver forebygging. De viser også til en sammenheng mellom teknologi og sosial kontroll. Byrne og Marx (2011, s. 18) mener at vi i dag i økende grad bruker hard teknologi i den hensikt å skulle forhindre kriminalitet. Eksempler på dette er overvåkningskameraer, metalldetektorer, sikkerhets- og bagasjekontroller på flyplasser, ulike sikkerhetssystemer og teknologiforbedrede patruljebiler. Et utvalg av slike harde teknologier vil i analysen trekkes frem i informantenes intervjuer. Myk teknologi involverer strategisk bruk av informasjon for å forhindre kriminalitet og for å forbedre politiets ytelse. Eksempler på dette er risiko- og trusselvurderinger, ulike programvarer, klassifiseringssystemer, profilering, ansiktsgjenkjenningsprogrammer og kriminalitetsanalyser. Eksempelvis gir Politiets Sikkerhetstjeneste årlig ut trusselvurderinger, der de redegjør for trusselbildet som det norske samfunnet står overfor. I trusselvurderingen for 2023 skrives det følgende om trusselvurderingens målsetting: «Hensikten er å skape en bevissthet om de mest alvorlige truslene mot Norge og å gi beslutningsstøtte i det viktige forebyggende sikkerhetsarbeidet som virksomheter har ansvaret for» (PST, 2023, s. 2). Vi kan dermed tydelig se hvordan forebygging er et mål for norske myndigheter gjennom bruken av myk teknologi. Også flere av de overnevnte myke teknologiene vil være sentrale for avhandlingens analyse. Informasjons- og materialbasert teknologi er i sum med på å fange opp spekteret av de ulike teknologiske innovasjoner, som politimyndigheter benytter i forebyggende øyemed.

Et sentralt eksempel på hvordan teknologien har fått innpass i politiets forebygging er det «forutseende politiarbeidet», som skal veilede politiet i deres forebygging, med utgangspunkt i kunnskapsbasert teknologi. Slikt prediktivt politiarbeid beskrives som «anvendelsen av analytiske teknikker; spesielt kvantitative, for å identifisere sannsynlige mål for politiintervensjon og forhindre kriminalitet» (Wilson, 2019, s. 72). Med andre ord handler dette om å forhindre kriminalitet eller løse tidligere lovbrudd ved bruk av såkalte statistiske spådommer. Det beskrives som et mål å bevege seg nærmest mulig sanntid i en slik forebygging (Byrne & Marx, 2011, s. 18). Vi kan gjenkjenne denne tendensen i flere av de moderne forebyggende teknologiene politiet benytter i dag. Elementet av å skulle handle «forut hendelsen», er en del av det som skiller det forutseende politiarbeidet fra tradisjonell forebygging (Chan & Moses, 2018, s. 808). Teknologiens inntreden i politiets kriminalitetsforebygging er dermed sentral for å forstå dagens fremtidsrettede politimandat.

Utgangspunktet er at forebygging ved bruk av teknologi skal hjelpe politiet med sine arbeidsoppgaver (Byrne & Marx, 2011, s. 17). Likevel finner vi i forskning ulike tilnærminger til den prediktive og teknologiske forebyggingen. Byrne og Marx (2011, s. 17) mener at vi vet lite om forklaringsmodellene bak mange forebyggende teknologier. De viser også til lite kunnskap om både de tilsiktede og utilsiktede konsekvensene av dem. Janet Chan (2021, s. 50) mener at det selges en utopisk visjon om prediktivt politiarbeid. Chan begrunner dette med eksisterende karakteriseringer og eksemplifiserer med følgende beskrivelser: «faktabasert», «risikobasert», «et paradigmeskifte i rettshåndhevelse» og «en betydelig forbedring av politiets resultater gjennom informasjonsbasert taktikk, strategi og politikk». Chan mener at slike forestillinger gir en urealistisk fremstilling av prediktiv teknologi. Perry, et. al. (2013, referert i Chan, 2021, s. 50) beskriver på sin side myter de setter i sammenheng med forutseende politiarbeid. For det første viser de til en utbredt formening om at prediktivt politiarbeid tolkes dithen at datamaskiner kan forutsi fremtiden eller at slikt politiarbeid er en «krystallkule». I realiteten viser de til at programvaren kun er i stand til å forutsi *risikoen* for fremtidig kriminalitet, samt at spådommer bare er så gode som de underliggende dataene er. De viser også til myten om at datamaskinen «kan gjøre alt for deg», på tross av at mennesker er en helt avgjørende part i det prediktive arbeidet. Et viktig poeng er nettopp at forebyggende teknologi vil være avhengig av mennesker. Konsekvensen er at forebyggende teknologi vil være menneskepåvirket. Hvordan en slik menneskelig påvirkning virker inn på teknologien, har dermed vært et viktig aspekt å undersøke i avhandlingen.

2.3 Kunstig intelligens og maskinlæring

Vi har hittil sett på hvordan politiets tilnærming til forebyggingsbegrepet legger føringer på hvordan deres arbeidsoppgaver utøves. Det er også beskrevet hvordan teknologien har gjort seg relevant innenfor kriminalitetsforebygging, gjennom å fremme effektivisering og muligheten til å drive proaktivt politiarbeid. Det er samtidig eksemplifisert de ulike teknologier som benyttes av politiet i dag. I dette delkapittelet vil det gjøres en avklaring rundt hvordan slik forebyggende teknologi er bygd opp.

Den forebyggende teknologiens utgangspunkt er å være i forkjøpet av en hendelse eller et lovbrudd. Politiet bruker i økende grad fremskritt innen datavitenskap og statistikk til slike formål (Vestby & Vestby, 2019, s. 1). Anvendelsen av maskinlæring (Vestby, 2018, s. 4),

kunstig intelligens (Chan, 2021, s. 48) og algoritmebasert teknologi (Leese, 2014, s. 494) har vært en sentral del av en slik utvikling.

Algoritmer blir forstått som generaliserte prosedyrer for å gjøre uorganiserte data-inputs til håndterbare data-outputs. Dette gjøres gjennom en rekke logiske regler som gir instruksjoner om håndteringen av denne typen data (Kommunal- og moderniseringsdepartementet, 2020, s. 10). *Stordata* beskrives på sin side som algoritmebaserte analyser i storskala, forskjellige digitale data for prediksjon, måling og styring (Flyverbom & Madsen, 2015, s. 142). Et dataprogram som gjør en bestemt oppgave kaller vi enkelt forklart for en algoritme. Når dataprogrammet klarer å løse en vanskelig oppgave, faller algoritmen innunder det vi omtaler som *kunstig intelligens*. Datamaskinalgoritmer er bygd opp på ulike måter. Den mest vanlige måten er når en programmerer bestemmer nøyaktige instrukser som algoritmen skal utføre. En annen måte å bygge opp algoritmer på, er å trene dem opp. Denne prosessen kaller vi *maskinlæring*. Maskinlæring er altså å anse som en prosess innenfor kunstig intelligens (Kommunal- og moderniseringsdepartementet, 2020, ss. 10-11). Flertallet av de kunstig intelligente algoritmene programmeres altså ikke, men lærer. Dette skjer ved at algoritmene trenes opp, gjennom å mate dem med informasjon. Med nok informasjon vil algoritmene selv kunne identisisere ulike mønstre (Goodwin, 2020, ss. 7-9). Systemer basert på kunstig intelligens kan få inn data fra ulike informasjonskilder. De kan også tolke data fra eksempelvis sensorer, kameraer eller mikrofoner. Systemene analyserer så dataene, tar beslutninger, og utfører deretter handlinger (Kommunal- og moderniseringsdepartementet, 2020, s. 10). Hensikten med slik teknologi er å oppnå gitte mål (Klepper, et al., 2021, s. 22). I denne avhandlingen vil det tas utgangspunkt i kriminalitetsforebygging som et slikt gitt mål.

Av forklaringen ovenfor kan vi se hvordan kunstig intelligens benyttes som et samlebegrep for en rekke ulike relaterte beregningsteknikker, behandlingssystemer og verktøy for problemløsning og utførelse av oppgaver som normalt krever menneskelig intelligens (Chan, 2021, s. 41). Kunstig intelligens er dermed overordnet maskinlæring. Dette gjør skillelinjene mellom KI og ML uklare. I denne avhandlingen vil hovedfokuset ligge på teknologi som både benytter maskinlæring og kunstig intelligens. Begrepene vil derfor brukes om hverandre, mens teknologi-terminologien er en en samlebetegnelse på de ulike digitale teknologiske verktøyene som brukes til kriminalitetsforebygging.

Kunstig intelligens er som nevnt i avhandlingens innledning et teknologiområde som det i dag rettes stor oppmerksomhet mot. Det vises til at denne typen teknologi har mange tiltenkte anvendelser i fremtiden. Mange bruksområder eksisterer allerede i dag. KI forventes å kunne bli brukt til stadig mer avanserte og automatiserte former for dataanalyse. Utgangspunktet er at slik teknologi kan bidra til at vi ser sammenhenger vi tidligere ikke var bevisst, og at det som tidligere har vært avhengig av manuelle prosesser kan automatiseres og forenkles (Klepper, et al., 2021, s. 22). Som også beskrevet innledningsvis har oppmerksomheten rundt kunstig intelligens det siste halvåret gjort seg spesielt gjeldende gjennom OpenAI sin tjeneste «ChatGPT» (Generative pre-trained transformer). Dette er et dataprogram i form av en chatbot. Chatboten er programmert til å besvare spørsmål og løse problemer. For å gjøre dette bruker teknologien maskinlæring av språkmodeller til å produsere tekst (Eriksen, 2022). Bruken av ChatGPT har spredd seg verden over, og benyttes daglig av millioner av mennesker. Det har samtidig blitt stilt spørsmålstegn ved begrensningene til teknologien, og hvor intelligent vi faktisk ønsker at den skal bli (Knudsen, 2023). En rekke navngitte personer som arbeider med kunstig intelligens har vist til behovet for å pause utviklingen, for å forstå mer om teknologien og risikoen den kan inneha (Future of life Institute, 2023). Dette er i tråd med forskning som peker på etiske og juridiske problemstillinger som vil oppstå dersom kunstig intelligens får «løpe fritt» i samfunnet. Datadrevne skjevheter, problemer med tillit til teknologi og mangelen på gjennomsiktighet trekkes frem som eksempler på dette (Chan, 2021, s. 47).

Mye av styrken til kunstig intelligens ligger nettopp i at teknologien kan lære på egenhånd, samt at den gradvis vil forbedres og få utvidede bruksområder. I det langsiktige perspektivet kan såkalt avansert kunstig intelligens føre til at teknologien mer eller mindre kan etterligne menneskelige tankesett og agere på egenhånd (Klepper, et al., 2021, s. 22). På denne måten vil KI også fremme kompleksitet og sårbarhet i samfunnet. Et sentralt spørsmål i avhandlingen er hvor utbredt bruken av kunstig intelligente verktøy er i norsk politi i dag. I min tilnærming til fagfeltet, vil også et relevant spørsmål være hvilke holdninger informantene har til bruken av KI innenfor kriminalitetsforebygging.

Et viktig prinsipp skrevet i Nasjonal strategi for kunstig intelligens (Kommunal- og moderniseringsdepartementet, 2020, s. 59) er følgende: «KI-systemer skal legge til rette for inkludering, mangfold og likebehandling». Et sentralt spørsmål er hvordan dette skal la seg gjøre i realiteten. Tidligere digitaliseringsminister Nikolai Astrup har uttalt følgende:

> Det er ikke til å komme utenom at kunstig intelligens også reiser noen vanskelige spørsmål: Hvem har ansvaret for konsekvensene av en beslutning som er truffet av KI? Hva skjer når autonome systemer tar egne beslutninger som vi ikke er enige i og som i verste fall fører til skade? Og hvordan sørger vi for at teknologien ikke viderefører og forsterker bevisst og ubevisst diskriminering og forutinntatthet? (Kommunal- og moderniseringsdepartementet, 2020, s. 2).

Jeg mener at dette tydeliggjør viktigheten av å se nærmere på hvordan det på best mulig måte kan skapes tillitsfull teknologi i Norge i dag. Jeg er også opptatt av hvordan denne teknologien skal se ut og hvilken type kriminalitet den skal forebygge. For at kunstige intelligente systemer skal kunne legge til rette for likebehandling, forutsetter dette en forskningsmessig nøytralitet og objektivitet. Likevel vil det som forskning har vist til, finnes selektive mekanismer bak slike systemer. Det er interessant å undersøke hvilke mekanismer informantene har fokus på. Dette vil dermed være relevant tematikk i avhandlingens analyse. I min tilnærming til det teknologiske fagfeltet, vil det være viktig å se nærmere på både de positive og negative implikasjoner som kunstig intelligens fører med seg. Begge deler vil være viktige for å besvare avhandlingens problemstilling.

2.4 Implikasjoner av forebyggende teknologi

Kaufman, Egbert og Leese (2018, ss. 674-675) har skrevet om hvordan datapakker for prediktive analyser i økende grad blir implementert i politiarbeid i en rekke land. De beskriver hvordan disse datapakkene inneholder identifisering av bestemte mønstre som indikerer eller avskriver muligheten for lovbrudd. Dette vil i praksis si at slike forhåndstrukturerte algoritmer avgjør hvordan politiet skal arbeide og intervenere mot kriminalitet. På tross av at mønstrene i datapakkene er så avgjørende som de er, mener Kaufman, Egbert og Leese at de har fått relativt lite oppmerksomhet innad i litteraturen som omhandler kriminalitet og sikkerhet. De peker på at det gjerne har vært mest fokus på fordeler og ulemper ved en generell bruk av forutseende verktøy for kriminalitet.

I avhandlingen skal jeg undersøke nettopp det Kaufman, Egbert og Leese etterlyser innen kriminologisk forskning; de ulike aspektene, logikker og avgjørelser som inngår i produksjonen av slike mønstre.

Anette Vestby (2018) skriver i artikkelen «Policy making without politics: Overstating objectivity in intelligence-led policing» om forutseende verktøy som brukes av politiet. Hun peker på at den sosiale og teknologiske konteksten som denne typen verktøy befinner seg i, vil bestemme hvilken type informasjon som samles inn og hvordan denne typen informasjon blir oversatt og analysert. Vestby beskriver videre hvordan helheten av kriminalitet i et samfunn forblir uobservert, og at det kun er en andel av den som er kjent av politiet. Hvilken kriminalitet som faktisk observeres avhenger av hva politiet retter søkelyset mot. Politiets oppgave er å på best mulig måte maksimere skadereduksjon, og vil benytte seg av de forutseende verktøy de mener er i tråd med en slik målsetting. Vestby (2018, s. 268) trekker frem flere utfordringer ved en slik tilnærming til kriminalitetsforebygging:

> The crime problem currently identified and targeted may not be the one that is most harmful and/or cost- effective with regard to reducing harm. The 'usual suspect' isn't necessarily the most harmful possible suspect, and the systematic search for particular types of offences may result in selection bias.

Av Vestbys argumentasjon fremstår effektivt forebyggende politiarbeid som en subjektiv øvelse. Det er derfor interessant å undersøke hvorvidt forebyggende teknologi kan utvikles, implementeres og drives på en objektiv og nøytral måte. Vestby trekker også frem problematikk rundt skjeve modeller som vil kunne påvirke hvem som fanges opp av de forebyggende teknologiene. Vi kan av dette tolke Vestby dithen, at hun i likhet med Kaufman, Egbert og Leese mener at det som inngår i produksjonen av forebyggende teknologi er viktig å studere nærmere.

Med dagens teknologi benyttes det algoritmer som skal prosessere svært store mengder data. Matthias Leese (2014, s. 503) viser til at det oppstår flere potensielle problemstillinger i forbindelse med dette: For det første vil man risikere at teknologien opererer på egenhånd og på en måte som ikke er mulig for mennesker å forstå, diskutere eller etterprøve. Dette vil kunne skape såkalte «black boxes». I slike tilfeller vil det være svært krevende eller tilnærmet umulig å fastslå hvorfor maskinene har handlet på måten de har gjort. På denne måten vil bestemte personer eller grupper risikere å bli fanget opp av systemet, uten at det finnes noen konkret forklaring på hvordan eller hvorfor. I slike situasjoner vil det være risiko for at det oppstår problemstillinger rundt diskriminering og etikk (Leese, 2014, ss. 499-500). Dette er i tråd med Vestbys beskrivelser av potensielle skjeve modeller. Teknologi som i utgangspunktet skal forebygge, kan inneha åpenbare problematiske slagsider. En tolkning er dermed at

kriminalitetsforebygging ved bruk av teknologi kan ende opp med å virke mot sin hensikt. Dette har skapt et skille mellom de som mener at kunstig intelligens kan gjøre politiet smartere, og de som mener at vi bør være kritiske til KI-teknologier og de negative implikasjoner teknologien kan føre med seg (Chan, 2021, s. 48).

Et annet argument i forskningslitteraturen er at teknologien ikke kan gi en transparent og objektiv gjengivelse av virkeligheten: «Technologies do not deliver a transparent and objective rendition of reality. Rather, they play an active role in enacting it» (Niculescu-Dincă, 2021, s. 92). Dette er i tråd med det Fyfe, Gundhus og Rønn (2018, s. 150) beskriver i «Moral intelligence-led policing»: De viser til at prediktive programvarer ofte antas å være nøytrale eller objektive på bakgrunn av deres digitale, beregningsmessige og teknologiske karakter. Likevel vil prosessen med datautvelgelse være avhengig av ulike forståelser av kriminalitet. Fremtidige antagelser vil dermed ha utgangspunkt i historiske og rapporterte data. Dette vil også si at dataene er generert av noen; herunder politi, internettbrukere, administrative personer eller privatpersoner. Dette impliserer konsekvenser for kalkuleringen og prediksjonen av mønster i kriminaliteten (Fyfe, Gundhus, & Rønn, 2018, s. 150). Eksempelvis er kunstig intelligens avhengig av data som kan bli utnyttet til etiske tvilsomme formål. Det finnes derfor ingen garanti for at teknologien vil ha den tiltenkte effekten i samfunnet (Walsh, et al., 2019, s. 4, referert i Chan, 2021, s. 45).

Høyre har nylig vært ute og kritisert regjeringen for ikke å henge med på utviklingen av kunstig intelligens. De etterlyser samtidig en plan for bruken av KI i Norge. De viser til at fokuset må rettes mot to ulike aspekter: På den ene siden beskrives viktigheten av forskning på hvordan teknologien kan brukes til å løse oppgaver i offentlig og privat sektor på nye og bedre måter. På den andre siden understrekes kunnskapsbehovet for hvordan misbruk, spredning av feilinformasjon og diskriminering ved systematisk skjevhet i KI-systemer kan forhindres. Både kunstig intelligens nytte- og skadepotensiale er dermed relevant i en slik sammenheng. Linda Hofstad Helland i Høyre viser til følgende metafor: «Imens KI-toget går, står vi igjen på perrongen» (Solheim & Mematpoor, 2023).

Vestby og Vestby (2019, s. 1) stiller i sin artikkel følgende spørsmål: «How can we secure an open democratic debate about police use of predictive analytics when the techonology itself is a specialized area of expertise?». Avhandlingens hensikt er å åpne opp for en diskusjon rundt bruken av kriminalitetsforebyggende teknologi og holdninger til dette. Et viktig element er å

undersøke hvordan fagpersoner ser på en slik teknologibruk og hva som kreves for å skape en tillitsfull bruk av den.

3 Teoretisk rammeverk

Sammen med forskningsbidragene som er diskutert i kapittel 2, vil de aktuelle perspektivene jeg presenterer i dette kapittelet brukes for å sette avhandlingen i en teoretisk kontekst. Dette vil gjøres gjennom tre overordnende temaer: «diskurser av overvåkning», «sikkerhetsperspektiver» og «pre-kriminalitet». Det er viktig å påpeke at det finnes et stort utvalg av kriminologisk litteratur som kan belyse dagens kriminalitetskontroll. Jeg har selv valgt ut det jeg fant nyttigst for å forstå de underliggende diskurser til avhandlingens tematikk.

3.1 Diskurser om overvåkning

Zedner og Ashworth (2014, s. 11) beskriver den tydelige utviklingen av hvordan det forebyggende fokuset har vært i endring; de viser til at én måte å arbeide forebyggende på har vært å straffe kriminelle, plassere dem i fengsel og potensielt rehabilitere de mens de er satt bort av samfunnet. Dette har også kunne hatt en avskrekkende effekt på kriminelle og andre utenforstående. Dette er i tråd med Gundhus sin beskrivelse av den tradisjonelle forståelsen av forebygging som beskrevet tidligere. Ifølge Zedner og Ashworth, regnes ikke lengre dette som den mest effektive måten å drive forebyggende arbeid på: Staten kan også forsøke å identifisere og nøytralisere farlige individer *før* de begår lovbrudd. Dette gjøres gjennom å begrense friheten deres på ulike måter og er hovedtendensen i det som har fått navnet «den preventive staten». Zedner og Ashworth (2014, s. 11) stiller samtidig spørsmål ved hvor «preventiv» en slik tilnærming til kriminalitetskontrollen egentlig er, og om hvorvidt slike forebyggende tiltak egentlig er straffende.

Dette er et av hovedpoengene til Stanley Cohen i «The punitive city» (1979, s. 341). Der beskriver Cohen hvordan den sosiale kontrollen har vært i endring som følge av nye forståelser av hvordan man får lydige og kontrollerte individer. Hensikten var å motvirke den økte kriminaliteten som fant sted på 1960- og 70-tallet. Konsekvensen av dette var innlemmingen av regler og disiplin i de nye systemene for kriminalitetsforebygging. Dette førte til en såkalt «utvidelse av nettet» (Cohen, 1979, ss. 346-347). Her kontrollerte og sanksjonerte man ikke lengre kun de fengslede, men samfunnet generelt (Cohen 1979, s. 341). Cohen (1979, ss. 346-347) beskriver hvordan dette førte til en utvidelse i overvåkning, samt at flere kom inn i systemet på grunn av mindre alvorlige lovbrudd. Konsekvensen var at skillelinjene mellom fengsel og sivilsamfunn ble mindre, gjennom økt overvåkning og kontroll. Det ble dannet nye mønstre for sosial kontroll, og disse utviklet og spredde seg i samfunnet. Det medførte også at

det ble skapt nye avvikskategorier. Nye instanser utviklet egen ekspertise for sosial kontroll og kriminalitetsforebyggingen fantes i alle deler av samfunnet.

Cohen er inspirert av Michel Foucaults tankegang vedrørende overvåkning av befolkningen: Foucault (1999, s. 162) trekker paralleller mellom den panoptiske fengselsmodellen til Jeremy Bentham og utviklingen av overvåkningen av samfunnet. Det panoptiske fengselet hadde til hensikt å overvåke til enhver tid og skulle gjennom makt og disiplin kontrollere de innsatte. En slik panoptisme brukes som en metafor for hvordan det moderne samfunnet er under en konstant generalisert overvåkning. Dette er en sentral del av det Cohen beskriver i «The punitive city», der trusselen om overvåkning og straff legger grunnlaget for hvordan den sosiale kontrollen fungerer og disiplinerer samfunnet (Cohen, 1979, s. 347). Det er mulig å trekke paralleller mellom Cohens beskrivelser av panoptisme og teknologiutviklingen i dagens samfunn. Forebyggende teknologier fungerer som en konstant overvåkningsmekanisme som samfunnsmedlemmer må innrette seg etter.

Vi kan samtidig tydelig se hvordan Cohens beskrivelser av uklare skillelinjer mellom fengsel og sivilsamfunn er sammenlignbare med samfunnsstrukturene som finnes i dag. Den digitale tidsalderen kjennetegnes av at aktører innen både offentlige og private institusjoner i økende grad samler inn data om mennesker og atferd. Dette gjøres gjennom klassifisering, sortering og inngripen på ulike måter (Brayne, 2022, s. 372), samt ved at folk frivillig legger ut spor etter seg i sosiale medier og på ulike plattformer (Flyverbom & Murray, 2018, s. 4). Overvåkningen foregår derfor i alle sfærer i samfunnet.

Sarah Brayne (2022, s. 374) viser til at overvåkningsstudier ikke er et nytt fenomen og at stater alltid har sporet sin befolkning. Også befolkningen selv i et samfunn har over lengre tid fungert som ledd i en slik sporing. Hvordan amerikanske myndigheter i kjølvannet av 11. september 2001 lanserte følgende nasjonal oppfordring: «if you see something, say something», rettet mot den amerikanske befolkningen, er ifølge Brayne et eksempel på dette. Det som derimot er annerledes i dag, er hvordan overvåkningskapasiteten og omfanget stadig intensiveres som følge av teknologi. Teknologi er dermed med på å utvide rekkevidden for statlig overvåkning.

Diskurser om en preventiv stat settes altså i sammenheng med en «overvåkende stat». Thomas Mathiesen (2013, s. 133) mener at det har funnet sted en endring i både statens og markedets overvåkningskapasitet og behov for kontroll. Han mener at de mange systemene setter

menneskers privatliv og sivile rettigheter i fare (Mathiesen, 2013, s. 126). Mathisen (2013, s. 150) viser til at det opp gjennom årene har vært mange advarsler mot overvåkning generelt. Han trekker frem spådommer om at fremtiden kan være farlig og at det politiske demokratiske systemet i verste fall kan vakle og gå over til noe mer udemokratisk og autoritært. Han stiller spørsmålstegn ved om vi er i ferd med å utvikle en rettslig overbygning; et vidt utbredt, integrert og globalt kontrollsystem som eksisterer i og for seg selv, uten noen stat (Mathiesen, 2013, s. 102). Mathiesen (2013, s. 153) mener at vi ikke må tro at inngripende overvåkning ligger i fremtiden, men at fremtiden er nå.

David Lyon (2003, s. 1) definerer moderne overvåkning som en prosess for sosial sortering. Dette innebærer å dele grupper av mennesker inn i kategorier og tildele verdi eller risiko. Det beskrives som et middel for sortering av mennesker og derav også et middel for sortering av diskriminerende behandling (Lyon, 2003, s. 4). Kategorisk mistanke involverer eksempelvis innsamling av informasjon for å klassifisere individer i henhold til risiko. Prediktivt politiarbeid trekkes frem som et eksempel på en slik klassifisering (Byrne & Marx, 2011, ss. 23-24). Lyon (2003, s. 4) viser i likhet med Braynes (2017) nyere studie til at teknologiske fremskritt påvirker overvåkningen i samfunnet i dag. Lyon (2003, s. 40) beskriver samtidig kompleksiteten ved overvåkning; dess mer som skal forebygges, dess mer data må samles inn for å identifisere risiko. Dette vil kunne ha konsekvenser for menneskene som identifiseres som mulige risikobærere i samfunnet.

Ut ifra forskningen beskrevet i dette delkapittelet, vil det være interessant å undersøke hvordan informantene stiller seg til sammenhengen mellom forebyggende teknologi og diskurser av overvåkning.

3.2 Sikkerhetsperspektiver

Mareile Kaufman (2018) beskriver hvordan vi har sett et tydelig skifte i den forebyggende valensen. Både i europeisk og amerikansk kontekst er det en økende sammenveving av kriminalitetskontroll og sikkerhetspolitikk. Tradisjonelt har dette vært områder med ulike politiske ansvarsområder. Kaufman peker på at dette skiftet begynte på 1990-tallet, og særlig etter at «krigen mot terror» kom på dagsordenen i USA på begynnelsen av 2000-tallet.

Kaufman skiller mellom tre ulike perspektiver som beskriver hvordan diskurser av sikkerhet har beveget seg inn i kriminalitetskontrollen. Det vises først til et narrativt perspektiv som

omhandler sikkerhet og språk. Her forklarer hun at språket som sikkerhetsmyndigheter og media bruker, vil påvirke samfunnsdebatten og oppfattelsen av hendelser og fenomener. Kaufman trekker frem «fremmedkriger», «terrorisme» og «radikalisering» som eksempler på slike narrativ. På sikt vil slike narrativ kunne føre til spesielle sikkerhetstiltak som integreres i kriminalitetsforebyggingen. Hvordan sikkerhet kommuniseres, vil dermed påvirke kriminalitetskontrollen (Kaufman, 2018, ss. 23-24). Kaufman (2018, ss. 25-26) viser så til det praktiske perspektivet som omhandler sikkerhet og handling. Her illustreres det hvordan skillet mellom interne og eksterne oppgaver viskes ut og at det i sikkerhetsfeltet oppstår nye praksiser og samarbeidsformer på tvers av fagområder og profesjoner. Et slikt perspektiv utforsker altså ulike måter å håndtere sikkerhet på. Det tredje og siste perspektivet Kaufman trekker frem, er det materielle; sikkerhet og ting. Gjennom en slik tilnærming til sikkerhet forsøker en å forstå rollen som ting, utstyr og materiell spiller i sikkerhetspolitikken. Ting blir her ansett som redskap som skal beskytte samfunnet mot trusler. Kaufman viser til at dette spesielt gjelder teknologier. Eksempler som trekkes frem er overvåkningskameraer eller dataprogram for profilering av gjerningspersoner (Kaufman, 2018, ss. 27-28).

Det materielle perspektivet blir spesielt relevant når vi skal forstå bruken av forebyggende teknologi. Ulike teknologiske verktøy benyttes for opprettholdelsen av sikkerhet i samfunnet. Bruken av teknologi skaper ny praksis av lokal, nasjonal og internasjonal dimensjon, og kan være et ledd i kriminalitetskontrollen (Kaufman, 2018, s. 28). På denne måten kan vi se hvordan teknologi og forebygging settes i sammenheng gjennom et ønske om sikkerhet i samfunnet. Et slik materielt perspektiv vil falle inn under avhandlingens tilnærming til det forebyggende feltet.

Katja Franko (2013, s. 78) trekker på sin side en linje mellom sikkerhetsperspektiver og globalisering. Globalisering defineres som «intensiveringen av verdensomspennende sosiale relasjoner, som forbinder fjerne lokaliteter på en slik måte at lokale hendelser formes av andre hendelser som skjer langt unna, og omvendt» (Giddens, 1990, referert i Franko, 2013, s. 4). Franko (2013, s. 18) beskriver en fornyet tro på at stater skal håndtere kriminalitetsproblemer gjennom bruken av grensekontroll og økningen av statlig overvåkning. Hun viser her til økningen av straffende kontrollformer. I likhet med Zedner og Ashworth mener Franko at forebygging i dag innehar straffende aspekter. Franko (2013, s. 76) mener at globalisering har resultert i økende flyt av mennesker på tvers av landegrenser. Det har ført til behovet for en sterkere grensekontroll. Franko beskriver samtidig at en slik grensekontroll lager et skille

mellom territorier som skal beskyttes og territorier som skal ekskluderes. I sin tur vil dette også resultere i at bestemte grupper mennesker faller innunder de to ulike grupperingene (Aas, 2013, s. 79). Dette er tematikk som vil diskuteres nærmere i avhandlingen, der teknologi spiller en sentral rolle i grensekontroll. Politisering og migrasjonskontroll regnes som et av de mest definerende trekkene for nasjonal og internasjonal sikkerhet (Aas, 2013, s. 32). Lyon (2001, s. 90) siterer Anthony Giddens på at «å gjøre ting fra avstand er nøkkelen til å forstå den moderne verden».[2] Han viser til dette for å demonstrere den globale overvåkningen som praktiseres. Lyon (2001, s. 97) beskriver hvordan grenser i det moderne samfunnet både krysses fysisk og elektronisk. Lyon (2001, s. 90) mener dermed at vi kan snakke om en globaliserende forebygging; hvor ny teknologi muliggjør en global praksis. På bakgrunn av dette vil denne avhandlingen se nærmere på forebygging ved bruk av teknologi både i et nasjonalt og et globalt perspektiv.

Lucia Zedner (2009, s. 125) mener at sammenkoblingen mellom kriminalitet og sikkerhet har resultert i nye og alternative tilnærminger til kriminalitetsbekjempelse. Bruken av forebyggende teknologi trekkes frem som eksempel på dette. Zedner (2009, s. 125) viser også til at sikkerhetstiltak kan gå på bekostning av frihet og privatliv. Det vektlegges at tiltakene vil rette seg mot befolkningen generelt og ikke kun de som anses som åpenbare trusler mot samfunnet. Zedner setter dermed sikkerhet og overvåkning i sammenheng. I beskrivelser av sikkerhet og overvåkning i samfunnet, viser hun til hvordan forebyggingen handler om å sikre samfunnet *før* potensielle farer oppstår. Dette er i tråd med samfunnsutviklingen som er beskrevet tidligere i kapittelet. Det er samtidig også en sentral del av pre-kriminaliteten.[3] Dette er det siste teoretiske perspektivet som vil introduseres i gjeldende kapittel.

3.3 Pre-kriminalitet og foregripelse

Zedner (2007, s. 262) beskriver hvordan synet på kriminalitet har endret seg. Det har gått fra å være fortidsorientert til å være fremtidsorientert. Det fortidsorienterte synet har bakgrunn i modellen man fant i tidsrommet før 1990-tallet, der man så på årsaker for kriminalitet. Samtidig ble avvik ansett som noe unormalt og fokuset lå på lovbruddet, lovbryteren, offeret, etterforskningen, rettsaken og straffen. Til sammenligning kan vi snakke om pre-kriminalitet. Dette er synet vi har beveget oss mot i dagens samfunn, der kriminalitet blir sett på som et

[2] «"Doing things at a distance", is as Antony Giddens says, a key to understanding the contemporary world.»

[3] Pre-crime

faktum, en rutine og en mulighet. I denne modellen anses kriminaliteten som kalkulerbar, og noe som kan forebygges. Fokuset ligger på kriminalitetsmulighetene og ikke på selve lovbruddet. Sentrale stikkord innenfor dette fremtidsorienterte synet på kriminalitet er prevensjon og risikohåndtering (Zedner, 2007, ss. 262-263).

Heidi Mork Lomell (2012, s. 86) beskriver hvordan denne utviklingen påvirker kriminalitetsforebygging: I utgangspunktet er tendensen å tenke på straffbare handlinger som fullførte handlinger. I dag ser vi derimot en endring hvor lovbrudd er et resultat av en utvidelse i straffeloven. Disse lovbruddene faller ikke innunder de tradisjonelle lovbruddene, men er kriminaliserte forsøk på lovbrudd og planlegging av lovbrudd. På denne måten dannes det en preventiv sirkel rundt det primære lovbruddet (Zedner og Ashworth 2011, s. 285 referert i Lomell 2012, s. 86). I tillegg behandles disse som materielle lovbrudd i seg selv og frigjøres fra det primære lovbruddet. Kriminaliseringens legitimitet overføres dermed fra fullføring til forsøk (Lomell, 2012, s. 86).

Pre-kriminaliteten reflekterer en ny tilnærming til kriminalitet, risiko og fremtiden (McCulloch & Wilson, 2017, s. 36). I kriminalitetskontrollen resulterer dette i en utvidelse av politiets forebyggende mandat; potensielle trusler blir identifisert og håndtert gjennom menneskelig intervensjon, klassifiseringer og ulike teknologier (McCulloch & Wilson, 2017, s. 38). Pre-kriminaliteten anses i utgangspunktet som en spekulativ og usikker praksis. På motsatt side finner vi teknologi og vitenskap, som assosieres med presisjon, sikkerhet og nøytralitet. Når teknologien plasseres i en kontekst av pre-kriminalitet, vil pre-kriminaliteten kunne etterligne post-kriminaliteten. Det som i utgangspunktet kun er potensiell risiko, vil gjennom bruken av teknologi kunne fremstå som sikker kunnskap (McCulloch & Wilson, 2017, s. 76). Teknologi er på denne måten med på å opprettholde og videreutvikle denne nye tilnærmingen til kriminalitetsforebygging. En slik tilnærming til lovbrudd, er også med på å forme forebyggingsbegrepet og gjør det mer foregripende. Å handle *foregripende* innebærer at det gripes inn for å forhindre noe som er konstruert som irreversibelt eller som kan ha stort skadepotensiale. Dette vil også være tilfellet selv når trusselens spesifikke egenskaper er usikre (McCulloch & Wilson, 2017, s. 58).

Den foregripende teknologien hadde sitt inntog på begynnelsen av 2000-tallet og skulle forhindre nye terrorangrep før de forekom. Som følge av dette ble en rekke ulike teknikker for datainnsamling og overvåkning implementert i arbeidet for kontraterror. Disse teknikkene fløt

etter hvert også inn i den generelle kriminalitetsforebyggingen. Digitaliserte data, algoritmebaserte verktøy og prediktive analyser trekkes frem som eksempler på slik teknologi (McCulloch & Wilson, 2017, ss. 76-77). Vi kan se at dette er i tråd med Kaufmans observasjon av at sikkerhetspolitikk og kriminalitetkontroll har hatt en sammensmeltning. Konsekvensen av en slik tilnærming til forebygging, er at algoritmer i økende grad preger politiets praksis. En annen konsekvens er at samfunnsmedlemmer overvåkes i alle sfærer i livene sine. En slik omfattende overvåkning kan begrunnes i behovet for sikkerhet (McCulloch & Wilson, 2017, s. 83).

McCulloch og Wilson (2017, ss. 39-40) viser til at en slik tilnærming til kriminalitetsforebygging har sine slagsider. Det beskrives for det første som en selektiv praksis, der fokuset rettes mot noen typer lovbrudd og at man dermed risikerer å overse andre typer lovbrudd. Et annet sentralt element er at en slik risikobasert tilnærming til kriminalitet overser viktige sosiale og samfunnsmessige aspekter. Et tredje poeng som trekkes frem er risikoen for feilplassering av nødvendige ressurser i kriminalitetskontrollen. Teknologisk determinisme er en forestilling om at den teknologiske kunnskapen og de teknologiske løsningene i et samfunn er førende for hva slags samfunn som utvikler seg (Kjelsberg, 2022, s. 112). Av dette kan vi tolke det som at det er noe iboende ved teknologien, som påvirker samfunnet. Det vises til at et samfunn uten potensielle trusler og kriminalitet er en utopisk ønsketenkning (McCulloch & Wilson, 2017, s. 37). Hvor grensene for inngripende forebyggende teknologi skal gå, er dermed et sentralt spørsmål, både i avhandlingen og i kriminologien for øvrig.

4 Metode

Dette kapittelet vil redegjøre for avhandlingens metodiske grunnlag. Prosjektdesignmessige avgjørelser og vitenskapsteoretiske avveininger er herunder sentralt. Det vil først gis en presentasjon av kvalitativ metode. Dette vil gjøres for å belyse hvordan denne fremgangsmåten egner seg for å besvare avhandlingens tematikk. Videre vil utvalgs- og rekrutteringsprosesser beskrives. Etter dette vil prosessen rundt selve intervjuene utdypes. Til slutt vil forskningsetiske overveielser og etikk som dukket opp i arbeidet med prosjektet beskrives.

4.1 Kvalitativ forskning

Formålet med avhandlingen er å utforske erfaringer med teknologier for kriminalitetsforebygging, samt å undersøke hva som kreves for å tilrettelegge for en tillitsfull bruk av slike teknologier. For å undersøke dette har utgangspunktet vært å intervjue personer som har kjennskap til og inngående kunnskap om avhandlingens tematikk. På bakgrunn av dette er kvalitativ metode brukt som utgangspunkt for datainnsamlingen. Et av de fremste kjennetegnene ved kvalitativ metode er ønsket om å forstå verden fra perspektivet til individene vi studerer. Kvalitative forskningsmetoder er nyttige for å få en dybdeforståelse av ulike fenomener. Denne typen forskning kan brukes når hensikten er å forstå ulike prosesser, samt å identifisere sosiale, kulturelle, økonomiske eller fysiske kontekster (Hennink, Hutter, & Bailey, 2020, s. 11). Ut ifra definisjonen på kvalitativ metode, kan vi se at den er i tråd med formålet til denne avhandlingen.

4.1.1 Kvalitative intervjuer

Målet med kvalitative intervjuer er å skape en overføringsverdi til generaliserbarhet. Gjennom intervjuene kan jeg dermed peke på prosesser, sammenhenger og kategorier som gjelder flere (Skilbrei, 2021, s. 65). På bakgrunn av avhandlingens tema ble det tidlig i prosjektfasen fastslått at kvalitative intervjuer ville være en hensiktsmessig form for innhenting av data. Det kvalitative forskningsintervjuet har som utgangspunkt å skulle forstå verden sett fra intervjuobjektets perspektiv (Brinkmann & Kvale, 2018, s. 2). Ved å bruke intervju som forskningsmetode er det derved mulig å undersøke hvordan intervjuobjektene arbeider med eller er involvert i ulike teknologier for kriminalitetsforebygging. Det vil også være mulig å få en forståelse av deres holdninger til bruken av eksisterende teknologier eller teknologier under utvikling. Per i dag er mange teknologier for kriminalitetsforebygging fremdeles på utviklingsnivå i Norge. Dette kan vi også se er tilfellet for de teknologier som fremheves i

avhandlingen. Med utgangspunkt i valgt forskningsspørsmål, ville det derfor trolig vært utfordrende å velge en annen metode for innhenting av data.

May-Len Skilbrei (2021, s. 66) skriver at kvalitative intervjuer er en nyttig måte å kunne etablere bred kunnskap på; ved å se et fenomen fra forskjellige synsvinkler gjennom ulike fagpersoner sine perspektiver og fortolkninger. Intervjuer som forskningsmetode er dermed en sentral kilde til kunnskapsproduksjon. Kunnskapen skapes i samspill mellom forskerens spørsmål og informantenes drøftelser og svar (Brinkmann & Kvale, 2018, s. 24). Likevel kan det være viktig å påpeke at det også finnes ulemper ved valgt metode; kvalitative en-til-en-intervjuer fremmer kun individuelle enkeltstående synspunkt. Tilbakemeldinger eller interaksjoner fra andre vil derfor ikke forekomme. Dermed er det kun forskerens og informantens tolkninger som kommer til uttrykk i selve kunnskapsproduksjonen (Hennink, Hutter, & Bailey, 2020, s. 105). Dette gjør at selve utvalget blir en viktig faktor i forskningen.

4.1.2 Utvalg

Når vi skal velge ut og samle inn data, finnes det en rekke forhold som må avklares. Først og fremst er det viktig på forhånd å undersøke hvorvidt det er mulig å få tak i den kunnskapen vi er på letning etter. I denne avhandlingen er som nevnt kvalitative intervjuer valgt som metode for å besvare avhandlingens problemstilling. Dermed vil det neste som må avklares være om det er mulig å få tak i aktuelle intervjuobjekter (Furseth & Everett, 2020, s. 143). Spørsmålet om hvem man skal intervjue, handler om å identifisere et utvalg som kan bidra med den kunnskapen som forskeren trenger (Skilbrei, 2021, s. 121). Gjeldende prosjekt har bestått av syv informanter. Dette har vært en kombinasjon av personer som arbeider med teknologier for kriminalitetsforebygging på ulike måter. I oppstarten av prosjektperioden ble det tydelig at overvekten av de som jobber med forebyggende teknologi er ansatte innenfor polisære instanser. Innledningsvis i kapittel 2 så vi av politilovens § 1 at det forebyggende arbeidet er en sentral del av politimyndigheters arbeidsoppgaver.

Politiets virksomhetsstrategi (Politidirektoratet, 2020, s. 6) beskriver at forebygging kan skje både før, under og i etterkant av en kriminell handling. Likevel fremheves det i strategien at: «Ambisjonen er at politiet skal være i forkant av kriminaliteten. Dette forutsetter at politiet har en systematisk, planmessig og kunnskapsbasert tilnærming til forebygging». Denne tilnærmingen til forebygging gjennom teknologi er det hovedsakelig politiets egen IT-enhet (PIT) som i dag har ansvaret for. På politiets nettside skrives det at organisasjonen er pådriver for digitalisering og jobber med fremtidsrettet teknologi og utvikling (Politiet, u. å.). Derfor har

politiansatte med slik kompetanse vært en viktig del av utvalget i avhandlingen. I tillegg har også andre relevante informanter vært viktig å inkludere. Dette har vært øvrige politiansatte, samt forskere og fagpersoner som arbeider innenfor akademia med kriminologi, jus, forebygging, forutseende politiarbeid og andre typer analytiske stillinger. Flere av de arbeider direkte med innføring av ulike teknologier som skal kunne brukes i politiet. Samlet sett har dette gitt et variert utvalg med grunnlag for nyanserte perspektiver av avhandlingens tematikk.

I kvalitative studier opereres det ofte med et skille mellom å velge informanter på bakgrunn av å skulle få en bredde i erfaringer og å gjøre et strategisk utvalg for å dekke spesifikke erfaringer. Ofte vil de to skillene være sammenfallende. Dette er tilfellet i denne studien, hvor informantene er rekruttert bredt (Skilbrei, 2021, s. 122). Utgangspunktet har som tidligere nevnt vært at de på ulike måter er involvert med teknologier for kriminalitetsforebygging. I denne avhandlingen har kunnskap om valgt tema vært et viktig utgangspunkt. Dette handler om at teknologi innen kriminalitetsforebygging krever en viss kompetanse og faglig forståelse for å kunne diskutere. Når vi samler inn kvalitative data, må vi basere oss på et strategisk utvalg av informanter. Dette vil si at vi skal forsøke å sikre oss at utvalget er teoretisk representativt for det fenomenet eller de sammenhengene vi er opptatte av (Bukve, 2021, s. 217). Ved å ha et bredt utvalg som representerer flere yrkesgrupper innenfor kriminalitetsforebyggende teknologi, sikrer vi oss et nyansert utvalg som kan gi grunnlag for teoretisk representativitet.

4.1.3 Størrelse på og øvrige avveininger i forbindelse med utvalg

Det kan være en krevende øvelse å finne en passende utvalgsstørrelse innenfor kvalitativ forskning. Kvalitative studier har fokus på rikheten i selve dataene, fremfor antallet informanter i seg selv. Store utvalgsstørrelser er derfor ikke en målsetting (Hennink, Hutter, & Bailey, 2020, s. 220). Det finnes heller ingen fastsatte retningslinjer for størrelsen på utvalget i kvalitative studier. Likevel er det viktig å ha nok data til å faktisk kunne si noe om fenomenet en undersøker. Til sammen intervjuet jeg som nevnt ovenfor syv informanter, noe som var i tråd med det ideelle antallet intervjuer som på forhånd var forespeilet av meg og veileder. Dette handler om at det i dag er relativt få aktører som driver med teknologi for kriminalitetsforebygging og som sitter på denne typen kunnskap. På bakgrunn av dette har utgangspunktet vært at et slikt antall trolig kunne dekke feltet på en god måte.

Kvalitative metoder handler om å utforske få enheter som man undersøker grundig. Det er derfor viktig å ta utgangspunkt i en mengde data som er realistisk og overkommelig innen den gitte tidsfristen (Skilbrei, 2021, ss. 169-170). Først måtte jeg skaffe oversikt over feltet av

personer med kunnskap om bruken av teknologier innen kriminalitetsforebygging. Siden det var et relativt lite informantantall, var mulighetene gode for å gjøre grundige analyser av hvert enkelt intervju. En fordel med større utvalg er naturlig nok bedre muligheter for generalisering. En annen fordel med et større eller mer variert utvalg er muligheten det gir til å kunne sammenligne ulike grupper (Fekjær, 2022, s. 76). I denne avhandlingen ble en slik løsning lagt bort på grunn av prosjektets avgrensede størrelse og prosjektperiode. Dess større utvalg; dess mer tidkrevende vil en analyseprosess være. Det ble også gjort en avveining om at det gjeldende utvalget i seg selv kunne besvare prosjektets problemstilling på en god måte.

Det endelige utvalget besto av fire forskere og tre ansatte i politiet. Det var variasjon i stillingsnivåene til informantene, hvor noen arbeidet mer overordnet enn andre. Informantene hadde også ulike fagområder. Dette gjorde at intervjuene var nyanserte og ulike i tolkningen av avhandlingens tematikk. Tre av informantene var kvinner og fire var menn. Kjønnsmessig var det dermed en liten overvekt av menn. Dette var tilfeldig, og handlet kun om hvem som takket ja til å stille til intervju. Det ble sendt ut intervjuforespørsel til begge kjønn i like stort omfang. Aldersspennet i utvalget var også relativt stort, både i intervjuforespørslene og i det endelige utvalget.

Utvalget har liten variasjon i etnisitet. Det er vanskelig å si om dette har gitt utslag i innholdet til det innsamlede intervjumaterialet. Bakgrunnen til et individ vil alltid påvirke holdningene og verdiene til vedkommende. Dermed kan dette ha spilt inn i den tematikken som de ulike informantene har vært opptatt av i intervjuene, samt informantenes holdninger. Det er viktig å påpeke at manglende etniske variasjoner i utvalget er tilfeldig. Utvalget har utelukkende vært et resultat av hvilke personer som har blitt rekruttert gjennom valgte metoder. Dette metodeutvalget vil gjennomgås i neste avsnitt. Det er derfor mulig at et relativt ensidig etnisk utvalg handler om hvilke personer som arbeider innenfor det aktuelle fagområdet.

4.2 Rekruttering og intervjuguide

4.2.1 Rekruttering

Rekruttering av informanter ble i første omgang gjort via veileder. Veileder har i en lengre periode vært involvert i et forskningsprosjekt som heter AGOPOL. Prosjektet skal undersøke hvordan politiets bruk av kunstig intelligens, digital teknologi og private sikkerhets-/teknologi-/konsulentselskaper kan bidra til å endre politiets samfunnsmandat og praksis. I forbindelse med dette prosjektet hadde veileder kontakter innad i sitt forskningsmiljø. Rekruttering av

informanter kunne derfor i oppstartfasen gjøres gjennom utsendelse av intervjuforespørsel på e-post til personer som veileder visste hadde kjennskap til prosjektets tematikk. Intervjuforespørsler ble sendt ut til de aktuelle informantene, med vedlagt informasjon om prosjektet. Flertallet av de som ble kontaktet svarte, men det var også en andel av personer som ikke responderte i det hele tatt. Et fåtall henviste meg videre til andre aktuelle intervjukandidater som de trodde kunne besvare avhandlingens tema bedre. Personene som ble intervjuet, ble samtidig benyttet for rekruttering av nye informanter. Skilbrei (2021, s. 125) definerer dette som snøballmetoden; hvor forskeren utvider kontaktflaten sin i feltet ved å bruke de kontaktene en allerede har.

For innhenting av informanter ble det altså det benyttet en kombinasjon av formelle nettverk og snøballmetoden. Alle metoder for rekruttering har sine fordeler og sine svakheter. Derfor vil det å kombinere ulike metoder kunne minimere svakhetene (Hennink, Hutter, & Bailey, 2020, s. 200). Ved å bruke snøballmetoden alene kan forskeren eksempelvis ende opp med informanter fra kun én spesifikk gruppe med bestemte egenskaper og med kjennskap til hverandre. I tillegg vil snøballmetoden alene kunne være tidkrevende fordi man identifiserer en og en informant om gangen (Hennink, Hutter, & Bailey, 2020, s. 214). Ved også å benytte andre metoder for rekruttering kan forskeren dermed oppnå et mer nyansert utvalg av informanter. På grunnlag av veileders kjennskap til potensielle informanter, samt kontaktene informantene har gitt videre til meg, tror jeg at jeg har klart å få tak i kjernen av de som jobber med kriminalitetsforebyggende teknologi. Prosjektet har dermed oppnådd en god oversikt over kompetansen på fagfeltet i Norge.

En vanlig utfordring med intervjustudier er at det er mer krevende å få tak i informanter enn forutsett (Skilbrei, 2021, s. 125). I denne avhandlingen fikk jeg informanter fortløpende gjennom høsten, med varierende mellomrom mellom intervjuene. I noen perioder kunne denne prosessen være stillestående. Der og da var det noe krevende og stressende, men i ettertid ser jeg at det var en fordel. Underveis i prosjektperioden dukket det opp nye momenter og vinklinger på avhandlingens tematikk som ble aktuelt å se nærmere på. Dette var da mulig å gjøre i de resterende intervjuene. På denne måten fungerte utsettelser av intervjuer som en kontinuerlig refleksiv og flytende forskningsprosess.

4.2.2 Intervjuguide

En helt sentral del av forberedelsene i en intervjustudie er å konkretisere innholdet i intervjuet. Forskeren må med andre ord bestemme hvordan intervjuene skal legges opp. En spesifikk form for forskningsintervju er det «semi-strukturerte» intervjuet (Skilbrei, 2021, s. 127). Det er denne formen for intervju som er benyttet i gjeldende avhandling. Hovedspørsmålene var nedskrevet på forhånd, sammen med eventuelle oppfølgingsspørsmål som kunne stilles der det var naturlig underveis i samtalen. Dette gjorde det mulig å sammenligne svarene fra de ulike informantene da materialet skulle analyseres. Alle fikk dermed de samme overordnede spørsmålene, men ulike oppfølgingsspørsmål. Dette gjorde intervjuene mer flytende, og medførte trolig at intervjuene føltes mer naturlige enn det et strukturert intervju ville gjort. For min egen del opplevdes det mer som en faglig samtale, hvor det også ga nytteverdi å få svar på spørsmålene som dukket opp underveis i intervjuet. I tillegg kunne jeg i intervjuene plukke opp sentrale poenger som informantene kom med og bygge videre opp under dem.

I de aktuelle intervjuene ble det stilt innledningsspørsmål som handlet om hva informanten arbeidet med. Dette ble en naturlig åpning i intervjuene, hvor informanten kunne fortelle litt generelt om sin tilnærming til avhandlingens tematikk. Ut over i intervjuet ble det mer naturlig å stille mer dyptgående spørsmål som handlet om informantens holdninger til teknologi og om hva som ville kreves for tillitsfull bruk av teknologi. Her var det også viktig å diskutere ulike spesifikke teknologier som kunne inkluderes i analysedelen av avhandlingen. Utgangspunktet var å holde spørsmålene så åpne som mulig underveis i intervjuene. Dette hadde flere fordeler. For det første kunne det legges til rette for informantenes egne refleksjoner. Samtidig kunne samtalen bli styrt dithen informanten selv syntes det var viktig. Til slutt var et poeng med å stille åpne spørsmål, også å unngå at det som ble spurt om var ledende i en eller annen retning (Skilbrei, 2021, s. 128). Mot slutten av alle intervjuene ble informantene spurt om det var noe de mente var viktig å ha med i intervjuet som ikke var blitt snakket om. Alle informantene responderte på dette på en eller annen måte. Enkelte av informantene brukte muligheten til å utbrodere temaer som allerede hadde blitt snakket om tidligere i intervjuet. Andre trakk frem nye ståsted eller perspektiver som ikke hadde blitt snakket om i det hele tatt. Begge formene for respons var nyttige for prosjektet i analyseprosessen.

I forkant av intervjuene ble det sendt et informasjonsskriv, et samtykkeskjema og diverse annen informasjon knyttet til prosjektet til informantene på e-post. Informasjonsskrivet inneholdt forskningens formål, innhold og metode. På denne måten kunne informantene sette seg inn i

hva intervjuene kom til å handle om. Det gjorde det samtidig mulig for dem å gjøre seg opp noen tanker i forkant av møtet. Også opplysninger om at deltagelse var frivillig og at deltagerne kunne trekke seg når som helst i forskningsprosessen var viktig å ha med i informasjonsskrivet (Skilbrei & Haugen, 2021, s. 59). Intervjuguide, informasjonsskrivet som ble oversendt til informantene og prosjektgodkjenning fra NSD ligger i avhandlingens vedleggsliste.

4.2.3 Intervju med eksperter og fagpersoner

Noe som skiller dette prosjektet fra en rekke andre kvalitative prosjektstudier er utvalget for datainnsamlingen. Som beskrevet innledningsvis i metodedelen var informantene i denne studien ansatte i politiet, forskere og andre fagpersoner på det aktuelle fagfeltet. Det er et viktig skille mellom et slikt utvalg og et utvalg som eksempelvis hadde bestått av elever i en videregående klasse eller ofre for en bestemt type lovbrudd.

Et såkalt ekspertintervju er en form for intervjumetode som jevnlig blir brukt innen forskning. Det defineres som et intervju med mål om å samle inn data om et spesifikt felt av interesse. Intervjuet har dermed fokus på informantens kompetanse på det aktuelle fagområdet. Eksperter defineres som «personer som er ansvarlig for utvikling, implementering eller kontroll av en løsning, eller personer som har privilegert tilgang til mennesker eller beslutningsprosesser» (Döringer, 2021, s. 266). Et slikt intervju kan beskrives som et teorigenererende intervju. Dette vil si at ekspertene er personer som innehar en bestemt status eller som utøver en funksjon i bestemte beslutningsprosesser, innenfor et fagfelt. I praksis betyr dette at deres kunnskap er med på å forme og bestemme et handlingsfelt. Som følge av dette vil ekspertkunnskapen ha en samfunnsrelevant dimensjon (Döringer, 2021, s. 267).

Det teorigenererende ekspertintervjuet har et analytisk og fortolkende perspektiv. Gjennom et slikt perspektiv kan det skisseres sammenhenger i empirien og utvikles teoretiske tilnærminger. Subjektive relevanser, synspunkt eller perspektiver som informantene trekker frem er derfor sentralt (Mergel, Edelmann, & Haug, 2019, s. 4). Hensikten i dette prosjektet har vært å samle inn data fra de som sitter på dybdekunnskap om bruken av teknologier innen kriminalitetsforebygging. Å benytte seg av ekspertintervju har resultert i at jeg har fått en forståelse for hvordan det kriminologiske landskapet på det aktuelle fagfeltet faktisk ser ut.

I prosjektet besto flere av spørsmålene av tekniske begreper og definisjonsspørsmål. Det var viktig å få informantene til å selv definere og avgrense de ulike begrepene. Underveis i

intervjuene etterspurte jeg eksempelvis informantenes egne definisjoner av kunstig intelligens og maskinlæring. På denne måten var det enklere å sette seg inn i hvordan informantene tenkte rundt temaene som ble omsnakket.

4.3 Datainnsamling og databehandling

4.3.1 Datainnsamling

Intervjuene ble gjort på utvalgets premisser, slik det passet utvalget best. Det ble derfor inngått en dialog med hver enkelt informant om hva som var den best mulige måten å gjennomføre intervjuet på. Bakgrunnen for dette var at de aktuelle informantene skulle finne det enklest mulig å takke ja til å bli med på prosjektet. All kommunikasjon som angikk intervjuene, ble gjort via e-post. Under selve intervjuene ble det lagt til rette for å møte informantene ansikt til ansikt. Dette var i utgangspunktet en ønskelig og hensiktsmessig situasjon for et intervju. Fire av informantene møtte opp på IKRS (Institutt for kriminologi og rettssosiologi). Det var på forhånd reservert et rom for intervjuene. En av informantene foretrakk å bli intervjuet på sin arbeidsplass. Her hadde personen organisert det slik at intervjuet ble avholdt på et privat rom. Grunnet sykdom og andre årsaker ble to av intervjuene holdt over videosamtaler på nettet. I disse tilfellene satt jeg i egen leilighet uten andre til stede. Heldigvis var verken faktorer som dårlig internettforbindelse, bakgrunnsstøy eller andre tekniske problemer en utfordring i noen av intervjuene.

Det var varierende når informantene hadde mulighet til å stille til intervju. Enkelte ga klarsignal på at de kunne stille allerede dagen etter at de hadde takket ja til intervju-invitasjonen. Andre hadde først mulighet til å stille flere måneder etter at de takket ja. Det ble i forkant av intervjuene gitt en anslått tid for hvor lang tid det kom til å ta. Derfor var det ønskelig å ikke bruke mer enn den fastsatte tiden. Det ble beregnet omtrent en time til hvert av intervjuene, hvor de fleste lå på mellom 50 og 60 minutter. Ett intervju varte i én time og 10 minutter.

Før selve intervjuet startet var det en innledende samtale med informanten. Her spurte jeg om informanten hadde noen eventuelle spørsmål. I tillegg ble det gitt noe praktisk informasjon om prosjektet. Dette er av Kvale og Brinkmann (2018, s. 62) definert som en «briefing». Her var det også viktig å spørre informanten om de hadde lest gjennom informasjonsskrivet for prosjektet. Etter at dette var avklart, ble informantene spurt om de var klare for å sette i gang selve intervjuet og starte lydopptaket.

Intervjuet ble tatt opp med opptaker lånt av UiO. Praktisk sett fungerte dette ved at diktafonen ble skrudd på rett før intervjuet startet. Den ble så liggende midt på bordet vendt mot informanten. I intervjuene over nett ble diktafonen lagt ved siden av dataen. Informanten ble informert om både når diktafonen ble skrudd på og når den ble skrudd av. På denne måten kunne informantene ha kontroll over hva opptaket av dem faktisk inneholdt. Opptakene fungerte som de skulle på alle intervjuene. Dette gjorde at samtlige intervjuer var av god kvalitet og kunne brukes i prosjektanalysen. Det ble heller ikke behov for å gjennomføre noen av intervjuene på nytt. Dette var det flere av informantene som uoppfordret sa at de var villige til å gjøre om det skulle vise seg at opptakeren ikke hadde fungert som den skulle. For egen del var det også viktig å dobbeltsjekke at opptakeren fungerte som den skulle dagen før hvert enkelt intervju, samt rett før intervjuet skulle finne sted. På denne måten var det mulig å avdekke potensielle problemer med opptakeren i forkant av intervjuene.

Alle informantene var vennlig innstilte og ga gode og utfyllende svar på spørsmålene som ble stilt i intervjuene. Dette var nok fordi alle informantene har relevante yrker for prosjektets tema. Siden informantene snakket om det de jobber med, satt de på mye relevant kunnskap. Mange av refleksjonene de gjorde i intervjuene var også problemstillinger de hadde vært innom i jobbsammenheng tidligere. Det ble heller ikke stilt personlige spørsmål eller snakket om samtaleemner som var utgangspunkt for personlige opplevelser eller sensitive utleveringer. Informantene var utelukkende engasjerte i prosjektet og ønsket å bidra så godt de kunne. Personer som arbeider innenfor spesifikke fagfelt, vil trolig gjerne være med på å bidra til økt kunnskap om fagfeltet sitt. Dette nevnte også flere av informantene selv. I tillegg nevnte flertallet av informantene at de hadde tidligere erfaring i å bli intervjuet i lignende sammenhenger. Jeg opplevde å få gode og detaljerte svar på de fleste spørsmålene. Dette ga meg mye materiale å analysere. De fleste var også opptatt av å hjelpe til videre i prosjektet ved å foreslå andre jeg kunne kontakte eller å bidra med ulike artikler eller annen type forskning jeg kunne undersøke videre. Jeg opplevde også at de var interesserte i prosjektet og i mine tanker rundt avhandlingens tematikk. Dette ble i noen av tilfellene diskutert etter at selve intervjuet var avsluttet. Hvis eventuelle spørsmål dukket opp underveis og i etterkant, var dette i meldingsutveksling over e-post.

4.3.2 Databehandling og analyse

Selve transkriberingen ble gjennomført ved å koble diktafonen med lydfiler til datamaskin via USB. Lydfilene ble så kopiert til datamaskinen for transkribering. Etter dette ble det

transkriberte opptaket slettet permanent, fra både diktafon og datamaskin. Det ble underveis i transkriberingen brukt kodenavn på hver av informantene. Elektroniske notater kan både inneholde sensitiv informasjon og inneholde informasjon som kan røpe identiteten til informantene. Det var derfor viktig å benytte praktiske måter for oppbevaring av materialet som var i tråd med forskningsmessig lovverk (Skilbrei, 2021, s. 173).

Intervjuene ble transkribert fortløpende. Transkribering er generelt ansett som en tidkrevende prosess. Det opplevdes derfor som hensiktsmessig å fordele denne arbeidsmengden utover prosjektperioden. Det var også nyttig å gjøre dette mellom hvert intervju siden jeg da kunne fange opp hva som kunne gjøre annerledes og forbedres til neste intervju. Dette kunne eksempelvis være måten spørsmål ble formulert eller rekkefølgen spørsmål ble stilt på. I tillegg ble det enklere å plukke opp temaer og synspunkter som kunne inkluderes i neste intervju. Transkriberingen ble gjort uten noen form for egnet dataprogram, selv om dette ofte er et verktøy som benyttes innen forskning (Skilbrei, 2021, s. 173). Dette handlet hovedsakelig om at det forelagte materialet ikke var så stort at det ble ansett som problematisk å gjøre transskriberingen manuelt.

Prosessen videre handlet om å tolke, sortere og analysere datamaterialet. En slik fremgangsmåte kalles koding (Skilbrei, 2021, s. 171). Fra et metodologisk perspektiv kan koding hjelpe forskeren med å finne mønstre i et datamateriale (Skilbrei, 2021, s. 183). Kodingen i mitt prosjekt startet på mange måter allerede underveis i intervjuprosessen. I intervjuene var det mulig å fange opp spesifikke temaer og synspunkter som gikk igjen. Dette ble notert ned etter hvert. De gjennomgående temaene i datamaterialet ble dermed omgjort til koder. Noen koder var også koblet opp mot avhandlingens problemstilling. Disse kodene var dermed etablert allerede i forkant av intervjuene og tok hovedsakelig utgangspunkt i teorilesning. De fleste kodene ble likevel til i etterkant av transkriberingen. Kodingen fungerte på mange måter som en sorteringsprosess. Jeg valgte å benytte meg av fargekoding i tekstbehandlingsprogram. De ulike fargekodene var knyttet til spesifikke temaer som gikk igjen i intervjuene. Etter denne grovsorteringen av fargede kodemapper ble dataene i hver av de kodede fargemappene delt inn i underkategorier. Dette forenklet arbeidet med å skulle trekke ut sentrale elementer i hvert av intervjuene, og bidro til at det var mulig å sammenligne intervjuene på tvers av hverandre. Alt i alt gjorde kodingen analyseprosessen oversiktlig og strukturert for min egen del.

Analysen i avhandlingen ble gjort tematisk, ved å se på de likheter og ulikheter kodingen av informantenes intervjuer resulterte i. Siden flere av intervjuene hadde noen ikke-planlagte oppfølgingsspørsmål som viste seg å være interessante og relevante for studien, fikk dermed noen av dem også plass i analysen. Jeg har samtidig benyttet meg av en induktiv tilnærming til prosjektet, ved å trekke slutninger fra et utvalg av enkelttilfeller og til en populasjon. Induktiv forskning er ansett som en viktig del av vitenskapelig kunnskapsutvikling (Bukve, 2021, s. 65).

4.4 Forskningsetiske overveielser og etikk

Etiske avveininger er noe som må gjøres gjennom hele forskningsprosessen i et prosjekt fra start til slutt. Forskeren må derfor fatte refleksive valg ved måten forskningen gjøres på, samt være årvåken til kritiske og sensitive forhold som kan dukke opp underveis (Brinkmann & Kvale, 2018, s. 29). I mitt prosjekt har jeg forholdt meg til gjeldende retningslinjer i samsvar med NSD[4] og NESH[5]. Jeg vil nå trekke frem noen av de etiske avveiningene som har vært sentrale for meg.

4.4.1 Samtykke

Informert samtykke anses som en hjørnestein i forskningsetikken (Skilbrei & Haugen, 2021, s. 53). Dette belyser at informantene skal være tilstrekkelig informert om studien de deltar i. I dette prosjektet ble denne informasjonen formidlet gjennom et informasjonsskriv. Som tidligere nevnt mottok informantene dette skrivet som e-post i forkant av intervjuet. Her ble det gitt generell informasjon om studien. Før selve intervjuet ble satt i gang, spurte jeg informantene om de hadde lest gjennom informasjonsskrivet og om de godkjente innholdet. Ingen i prosjektutvalget skrev dermed under på samtykkeskjema fysisk, men ga muntlig bekreftelse på dette i lydopptaket i innledningen til hvert intervju. I informasjonsskrivet ble de også informert om hvordan informasjonen skulle behandles underveis og i etterkant av prosjektet.

Fritt samtykke forutsetter at informantene skal forstå at deltakelsen er frivillig. Forskningsdeltagerne skal med andre ord velge å delta uten å oppleve press som vanskeliggjør å si nei for dem. Dette har forskeren selv ansvar for å formidle. De skal også når som helst ha mulighet til å trekke seg fra prosjektet (Skilbrei & Haugen, 2021, s. 54). Praktisk sett ble dette gjort ved å oppgi min kontaktinformasjon i informasjonsskrivet. På denne måten kunne

[4] Norsk senter for forskningsdata

[5] National Committee for Research Ethics in the Social Sciences and the Humanities

informantene selv ta kontakt i prosjektperioden. Det ble også vektlagt at alle opplysninger om informantene ville bli slettet dersom de skulle ønske å trekke seg fra prosjektet.

Min egen erfaring var at kommunikasjonen i det store og hele fungerte greit. Likevel forekom det at flere av informantene brukte noe tid på å besvare intervjuforespørslene. Hos enkelte informanter var det også en utfordring at kommunikasjonen stoppet opp underveis etter flere e-post-utvekslinger. I alle tilfellene med manglende respons valgte jeg å sende en ny e-post for å følge opp. Dette resulterte i at noen intervjukandidater beklaget sent svar og etter dette sa seg villige til å stille til intervju. I et par tilfeller fikk jeg heller ikke respons på min oppfølgende e-post. Da valgte jeg å la være å sende enda en ny e-post, og heller finne nye potensielle informanter å kontakte. Jeg syntes det var en vanskelig balansegang mellom å være «frempå» og «masete». Dette var dermed den løsningen jeg var mest komfortabel med.

4.4.2 Konfidensialitet

Konfidensialitet innebærer at privat data som kan identifisere forskningsobjektene ikke skal anvendes eller rapporteres i prosjektet. Prinsippet er at de individene som deltar i forskningen har rett til privatliv. Konfidensialitet handler om at informasjonen som inngår i prosjektet begrenses til de som er autorisert til å ha tilgang til slik informasjon. Forskning på sensitive områder krever spesiell varsomhet (Brinkmann & Kvale, 2018, ss. 32-34). Gjeldende prosjekt har ikke omhandlet sensitiv tematikk eller behandlet spesifikke sensitive personopplysninger. Intervjuene har handlet om erfaringer med forebyggende teknologier, holdninger til teknologi og faglige refleksjoner rundt dette. Likevel har det naturligvis vært viktig å anonymisere informantene i prosjektet. Dette ble gjort allerede i transkriberingsfasen. I tillegg var det viktig å ikke skrive avhandlingen på en slik måte at spesifikke informanter var gjenkjennbare. I Norge er det et relativt lite fagmiljø på det aktuelle fagfeltet og dette gjorde anonymiseringen tidvis krevende. Noen av temaene i intervjuene måtte kuttes fra selve analysen for å forhindre at intervjuet kunne spores tilbake til en bestemt person. I tillegg ble samtlige informanter gitt fiktive navn i avhandlingen. All personidentifiserbar informasjon ble derfor fjernet.

Konfidensialitetskravet i gjeldende prosjekt innebærer som nevnt anonymisering av informantene. At informantene blir anonymisert vil si at identiteten deres holdes skjult. En konsekvens av dette som trekkes frem i metodelitteratur, er at informantene mister sin stemme i forskningen og derav sin autonomi. I praksis betyr dette at forskeren vil kunne ha fritt spillerom til å tolke det innsamlede intervjumaterialet, uten noen form for innblanding av

intervjudeltakerne. Objektivitet i tilnærmingen til datamaterialet er derfor svært viktig innenfor forskning. Informantene skal ikke føle seg misforstått eller at deres intervjuer blir tatt ut av sammenheng (Brinkmann & Kvale, 2018, s. 33). Dette kan forekomme både bevisst og ubevisst av forskeren. Bakgrunnen for dette er at forskeren bruker bestemte deler av et intervju for å forsterke egne argumenter eller poenger. På denne måten kan noe som i utgangspunktet skal beskytte informanten, brukes til forskerens fordel (Brinkmann & Kvale, 2018, s. 33). Skilbrei (2021, s. 178) viser til NESH sine forskningsetiske retningslinjer (§16). Her beskrives det hvordan det å ta hensyn til informantens egen forståelse er en viktig forpliktelse; forskeren skal bestrebe å forstå informanten, fremstille informantens tolkning på en rimelig måte, samt underbygge sine egne tolkninger godt.

For å ivareta dette ble alle intervjuer skrevet ned ordrett. Det var også viktig å analysere det informantene snakket om i lys av tematikken de faktisk snakket om. Det å ikke lete etter poenger som kun bekrefter egne antagelser er en kontinuerlig øvelse jeg hele tiden forsøkte å være oppmerksom på gjennom fortolkningsprosessen i prosjektet. Dette kan sies å være en del av det som inngår i forskerens rolle, som jeg nå vil gå nærmere inn på.

4.4.3 Forskerens rolle

Mitt siste forskningsetiske element omhandler forskeren selv. Forskerens rolle forutsetter moralsk integritet. I tillegg til å være kjent med etiske retningslinjer, er det også viktig å være bevisst det asymmetriske maktforholdet som kan oppstå i kvalitative intervjuer (Brinkmann & Kvale, 2018, s. 34). Dette opplevdes ikke som en stor utfordring i gjeldende prosjekt. Dette var nok mye fordi alle i utvalget var fagpersoner. Dette var også som tidligere nevnt personer som hadde tidligere erfaring med intervjusituasjoner. På mange måter var det også gjerne slik at informanten satt på mye kunnskap om det vi snakket om, noe som kan ha gitt informantene trygghet i intervjusituasjonen. Det fremsto ikke som at informantene forsøkte å svare på noen av spørsmålene på en bestemt måte. Dette kunne vært problematisk hvis informantene hadde trodd at det fantes «riktige» og «gale» svar til det de ble spurt om. Dette resulterte i at intervjusituasjonen for min egen del opplevdes som uanstrengt og naturlig.

Forskerrollen handler om å være så objektiv som mulig. Likevel er det en etablert sannhet at mennesker aldri vil klare å være helt nøytrale. Dette vil også gjelde innenfor kvalitativ forskning. Dette gjør at anerkjennelsen av subjektivitet innen forskning fremheves som viktig i kvalitative studier: «It acknowledges that the perspectives of study participants reflect their

subjective views of their social world, and that researchers also bring their subjective views of their influences to the research process (…)» (Hennink, Hutter, & Bailey, 2020, s. 64).

Å ha visshet om at min egen bakgrunn, mine emosjoner og min sosiale posisjon er en integrert del av prosessen i å produsere data, handler om å ha en fortolkende tilnærming til forskning (Hennink, Hutter, & Bailey, 2020, s. 65). Skilbrei (2021, s. 87) mener at man i gjennomføringen av kvalitative studier kan bruke refleksivitet som en styrke; ved å gjøre dette kan jeg som forsker ha en forståelse av hvordan jeg setter spor i egen forskning. Gjennom kriminologistudiet har jeg eksempelvis tillært meg kritisk tenkning. Dette har trolig hatt en innvirkning på hvordan jeg har tolket informantenes intervjuer. Det å tolke teknologier for kriminalitetsforebygging i lys av sikkerhetsperspektiver og kriminologiske teorier er også noe min faglige bakgrunn har resultert i. Til slutt vil jeg trekke frem at det å være ung kvinne kan ha hatt noe å si for hvordan informantene oppfattet meg som forsker. Kjønnsmessige dimensjoner vil i større og mindre grad virke inn i alle situasjoner og relasjoner. Likevel kan jeg ikke peke på noe som antydet at dette var tilfelle i prosjektet mitt.

5 Analyse

I dette kapittelet vil jeg se nærmere på funnene i avhandlingen, og diskutere dem i lys av teoretiske perspektiver og tidligere forskning. Analysen er delt inn i fem deler, og tar utgangspunkt i følgende temaer: «hvilken teknologi snakker vi om?», «fremtidsrettede syn», «hvem skal vi se til?», «utfordringer ved forebyggende teknologi» og «hvordan tilrettelegge for tillitsfull teknologi?».

5.1 Hvilken teknologi snakker vi om?

Som beskrevet innledningsvis vil avhandlingen ta for seg et flertall teknologier som er bygd på maskinlæring og kunstig intelligens. Dette handler om at prediktivt politiarbeid i økende grad knyttes opp mot automatiseringsprosesser hvor beslutningstaking gjøres på bakgrunn av dataanalyser (Fyfe, Gundhus, & Rønn, 2018, s. 143). Mange av dagens forebyggende teknologier er derfor basert på teknikker hvor vi ønsker å gi datamaskiner og dataprogrammer mest mulig intelligent respons. Mye av det informantene beskriver i intervjuene, er dermed arbeid eller forskning som omhandler KI og ML. Dette gir utgangspunkt for følgende spørsmål: Hvordan forstår de jeg har intervjuet maskinlæring og kunstig intelligens, samt eventuelle overlapp mellom dem?

De fleste informantene forstår kunstig intelligens som overordnet maskinlæring. Anne beskriver at maskinlæring er en del av paraplybegrepet «kunstig intelligens», der maskinlæringen er middelet til det man ønsker å oppnå med KI. Teknologien skal ligne på kognitive funksjoner som et menneske har, herunder evnen til å ta rasjonelle beslutninger og kunne se mønstre. Alt dette er ifølge Anne noe kunstig intelligens kan brukes til, med mange ulike midler for maskinlæring. Selv om bruken av kunstig intelligens er svært utbredt i samfunnet, understreker Anne at det per i dag brukes lite i politiet.

Også Bjørn beskriver hvordan kunstig intelligens og maskinlæring henger sammen. For ham er maskinlæring «mekanismen i en tjeneste som lages». Bjørn mener det er vanskelig å skulle definere kunstig intelligens. Bjørns tolkning er at det er et krevende skille mellom de to begrepene, og at det avhenger av hvilket arbeidsområde av teknologien vi befinner oss i. Han viser til at økonomer, jurister eller ledere høyere oppe i hierarkiet gjerne benytter seg av begrepet kunstig intelligens. Dette begrunner Bjørn på følgende måte:

> «Fordi det dekker masse teknologi som har veldig kompliserte og veldig subtile interaksjoner med alle ting og som påvirker personer masse, som er en stor sånn her lodden ball som er vanskelig å få tak i. Og da er det rett å si at istedenfor å avgrense og være helt presis, så tar vi en større sekk sånn at vi ikke risikerer at noe faller ut som egentlig burde vært med.»

Bjørn er altså opptatt av hvilket nivå man befinner seg på i forhold til teknologien: befinner vi oss på et mer overordnet plan som yrkesgruppene han viser til ovenfor, vil begrepet kunstig intelligens ifølge ham være dekkende for en rekke ulike teknologier. Arbeider man derimot med selve utviklingen og implementeringen av teknologi, vil det være nødvendig med mer konkrete og detaljerte beskrivelser av teknologiers oppbygning. I slike tilfeller vil skillet mellom maskinlæring og kunstig intelligens være viktig. Dette vil ifølge Bjørn avgjøre hvilket av begrepene man benytter seg av. Bjørn beskriver i likhet med Gro, at bruken av kunstig intelligens ikke er utbredt i norsk politi i dag.

For å skille mellom maskinlæring og kunstig intelligens, mener Gro at maskinlæring er veldig konkret; det er enkeltoppgaver eller flere oppgaver som blir effektivisert. Det påpekes at vi i denne sammenhengen må trå varsomt rundt skjeve data og såkalte «bias». Gro viser til at dette er «ganske rå teknologi» og trekker paralleller til «deep learning» og «deep fakes». «Deep learning» er evnen maskinen har til å lære og tilegne seg kunnskap (Chan, 2021, s. 47). «Deep fakes» er falske videoer og lydklipp laget av maskiner, som i dag kan være vanskelig å avsløre som falske (Teknologirådet, 2018, s. 11). Gro mener at den kunstige intelligensen handler om hvorvidt teknologien kan bli fullstendig intelligent.

Cato er i sine beskrivelser mer detaljert i sin forståelse av kunstig intelligens. Ifølge ham henger kunstig intelligens sammen med datadrevet læring. Det vises til at modellen for en analyse vil påvirkes av dataene du putter inn i den, såkalte input-data. Cato eksemplifiserer og sier at hvis du har store mengder data som du trener opp, vil du med maskinlæringsalgoritmer få en output basert på dataene du putter inn. Cato viser til problematikken som oppstår hvis det er store skjevheter i dataene. Konsekvensen er at resultatet også blir skjevt, fordi analyseelementet som ligger i midten vil påvirkes av disse input-dataene. Samtidig mener han at definisjonsavgrensningen er et stort og vanskelig spørsmål. For å skille mellom KI og ML viser Cato til at i maskinlæring «putter du inn en forhåndsdefinert algoritme». De stegene algoritmen går gjennom, skal sørge for at input- og output-dataene henger sammen. I motsetning til dette

mener Cato at den kunstige intelligensen er selvkorrigerende. Slike selvkorrigeringsmekanismer er ifølge ham sentrale i å skille de to begrepene fra hverandre.

På den andre siden vektlegger Dina at kunstig intelligens er datasystemer eller teknologi som utfører eller som kan utføre oppgaver som krever menneskelig intelligens. Hun påpeker at intelligensen i datasystemene dermed er kunstig, fremfor menneskelig. Mye av det som KI er tiltenkt, mener hun er beslutningsstøttende til det vi ikke klarer med egen intelligens. Dina viser til at KI kan brukes til å oversette språk, finne objekter på bilder eller estimere risiko. Dina gir disse eksemplene fordi de er ulike og innehar ulike metoder. Ifølge henne må mye av den kunstige intelligensen gjennomgås manuelt for å lete etter feil, men hun mener at den kan være et godt utgangspunkt for å løse en arbeidsoppgave. Dinas tolkning er at det er vanskelig å trekke et skille mellom KI og ML. Dette fordi hun mener at det ikke er to forskjellige ting: «Så jeg tenker at ML er en del av det som KI kan gjøre, eller at du bruker det til det». Dina påpeker så at det er «mye mer som går innunder KI enn under ML.»

I likhet med fremstillinger av kunstig intelligens og maskinlæring i forskningslitteraturen, så har de jeg har intervjuet vanskelig for å skille mellom de ulike formene for teknologier. Flere av informantene beskriver dermed et «flytende vannskille» mellom dem. I kapittel 2 av avhandlingen min ble det vist til at begrepene gjerne brukes om hverandre. Walsh, et al. (2019, referert i Chan, 2021, ss. 43-44) mener at det er manglende konsensus på en universell definisjon av kunstig intelligens blant fagpersoner som jobber med KI: «AI is not a specific technology, but a collection of interrelated technologies used to solve problems and perform tasks that, when humans do them, requires thinking».

Erik mener at KI tar utgangspunkt i prosesser hvor det finnes en viss grad av frihet i maskiner. Han korrigerer seg selv i intervjuet, og påpeker at han snakker om en tilsynelatende frihet. Den kunstige intelligensen ivaretar prosesser der vi normalt ville hatt mennesker til å gjøre vurderinger. For å skille mellom KI og ML viser han til at:

> «Du kan tenke deg KI som kun en algoritme som jobber på en nokså forutbestemt måte. Men hvis du introduserer ML i det, så tenker du at det er kunnskapsgrunnlaget som skal benyttes for den algoritmen, noe den algoritmen skal finne ut av på et vis. Så de henger tett sammen(...).»

Fredrik, som har datateknisk bakgrunn er også den som er mest teknisk i sine beskrivelser av KI og ML. Fredrik forklarer at utviklingen av kunstig intelligens startet allerede på 1950-tallet, og at KI er den «store boksen» hvor du kan «putte alt». Inne i denne boksen finnes maskinlæring. Han mener samtidig at det er en overlapp i begrepene. Fredrik tolker kunstig intelligens som et «flyktig begrep», men mener at KI handler om å «prosessere data på en måte som tradisjonell koding ikke kan gjøre». Maskinlæring definerer han som prosessen der vi trener maskinen og forteller den hva som er riktig og galt. På denne måten kan maskinen bli selvlært. Gjennom intervjuet fremmer Fredrik en tolkning av at kunstig intelligens og maskinlæring er i konstant utvikling og endring.

For å oppsummere første del av analysen, er det tydelig at det er en overlapp mellom maskinlæring og kunstig intelligens for informantene. Dette vil ha betydning for senere diskusjoner i avhandlingen. På bakgrunn av dette vil jeg gjennomgående i analysen drøfte forebyggende teknologi mer generelt. Jeg vil kun skille mellom begrepene dersom det er relevant for avhandlingens diskusjon. Et annet fellestrekk hos intervjudeltakerne er at de fremmer en kompleksitet i teknologien. De fremstiller den som både noe positivt og som noe potensielt negativt, på grunn av de mulighetene som finnes i kunstig intelligens og maskinlæring. De er også opptatt av teknologiens rekkevidde i samfunnet. Dette gjør det interessant å undersøke hvilke holdninger informantene har til fremtidens anvendelse av teknologi innenfor kriminalitetsforebygging.

5.2 Fremtidsrettede syn på teknologi

Sammenkoblingen mellom sikkerhet og bruken av teknologi har ført til en polarisert debatt. Kritikere viser til hvordan nye teknologier i verste fall kan resultere i et dystopisk og totalitært overvåkende samfunn (Lyon, 2001, s. 33). Begrep som «Big Brother» skal gi et bilde av hvordan staten er altseende overfor innbyggerne og hvor verden er inndelt i de som kontrollerer og de som blir kontrollert (Aas, Gundhus, & Lomell, 2009, s. 3). Utgangspunktet er at teknologier som skal sørge for menneskers sikkerhet, kan virke mot sin hensikt ved å skape usikkerhet. På den andre siden har man aktører som ser mulighetene for drastisk nedgang i kriminaliteten og mer effektiv politivirksomhet (Aas, Gundhus, & Lomell, 2009, s. 4).

På bakgrunn av dette har jeg vært interessert i å undersøke hvordan informantene personlig stiller seg til bruken av kunstig intelligens og maskinlæring innen kriminalitetsforebygging. Svarene fra de ulike informantene har vist seg å være varierte. Utelukkende alle informantene

veier i intervjuene både positive og negative sider ved utvikling og implementering av kriminalitetsforebyggende teknologibruk opp mot hverandre. Det som skiller informantene, er hvilke positive og negative momenter de vektlegger. Derfor vil første analysekapittel redegjøre for informantenes synspunkt og holdninger som gjør dem kritisk til fremtidens teknologi, samt deres synspunkt som gjør dem positive til bruken av teknologi for kriminalitetsforebygging. For å tydeliggjøre spekteret av informantenes holdninger, vil deres tolkninger bli plassert innunder tre kategorier; «teknologioptimisme», «teknologiens kompleksitet» og «et kritisk syn på teknologi».

5.2.1 Teknologioptimisme

Interpol mener at innovasjon er avgjørende for at politi- og påtaletjenestene skal kunne beholde sin posisjon mot kriminelle som kan utnytte nye teknologiske muligheter. Det pekes på et stadig mer komplekst trussellandskap (Klepper, et al., 2021, s. 9). Med lovbrudd som stadig forflytter seg til det digitale rommet, vises det til viktigheten av også å drive forebygging i det digitale rommet. Dette er noe flere av informantene vektlegger. Informantene viser til at teknologi har en rekke egenskaper som mennesker ikke har kapasitet eller evne til. Det blir eksempelvis trukket frem hvordan teknologi kan effektivisere forebyggende arbeid og finne mønstre som vi ellers ikke ville hatt evnen til å se. Dina mener at politiets forebyggingsmandat er helt avhengig av en teknologisk utvikling. På oppfølgingsspørsmål vedrørende hvilke typer lovbrudd teknologien kan bidra til å forebygge, svarer hun:

> «Ja, nå hørtes jeg jo veldig positiv ut når jeg sa «alt». Men jeg er jo åpen for det... men jeg har sunn skepsis, håper jeg. Så litt sånn optimistisk og forsiktig.»

Dina begrunner dette med å vise til hvor omfattende den teknologiske utviklingen er. På bakgrunn av dette mener hun at kriminalitetsforebygging ved bruk av teknologi kan «hjelpe litt på alt». Dina beskriver hvordan kunstig intelligens i dag har mange bruksområder i forebyggende arbeid; raskere informasjon, muligheten til å innhente informasjon som ikke ville vært mulig uten teknologi og utvikling av ulike analyser som tekstanalyser og geografiske analyser. Tekstanalyse forklarer hun at kan ta utgangspunkt i å spore potensielle lovbrudd på nett og dermed få informasjon som politiet på egen hånd ikke ville vært i stand til å sette seg inn i. Geografisk analyse er en form for prediktiv analyse som setter risiko og sikkerhetsstyring i sammenheng. London, Los Angeles, München, Philadelphia og Zurich er eksempler på byer hvor politiet bruker eller har testet slike programvarer. Hensikten er å forutsi hvor det er

sannsynlig at forbrytelser finner sted, eller hvem som sannsynligvis vil begå lovbrudd i fremtiden (Vestby & Vestby, 2019, s. 1). Bruken av kunstig intelligens i tekstanalyse og geografisk analyse er noe flere av informantene beskriver i intervjuene sine.

Dina argumenterer for et mer balansert syn på kriminalitetsforebyggende teknologi, der vi ikke utelukkende ser på de kritiske aspektene. Dina viser til det potensialet teknologi har og mener at hun selv «forsøker å ha en realistisk tilnærming som er optimistisk til alt teknologien kan hjelpe oss med».

Flere av informantene viser til at det finnes stor tillit til politiet i det norske samfunnet. Dette underbygges også av forskning: Norge beskrives som en nasjon med få innbyggere, god økonomi, relativ egalitet, små etniske og religiøse spredninger og lite vold og kriminalitet. Tilliten til politi, stat og rettsvesen regnes samtidig for å være blant den høyeste i verden (Larsson, Eriksen, Pedersen, & Alvin, 2022, s. 31). Egge, Strype og Thomasen (2012, s. 11) mener at den tilliten som finnes til politiet kan ha sammenheng med at Norge scorer høyt på den generelle tilliten i samfunnet. Samfunnstillit spiller inn når mennesker bedømmer politiet. Viktige kriterier for dette er forutsigbare, rettferdige og upartiske institusjoner. Det generelle inntrykket er at politiet har en høy og stabil tillit innad i Norge. Flertallet av informantene forteller at en slik tillit også preger måten teknologier utvikles og brukes på. Fredrik mener på sin side at tillit er komplekst. Dette begrunner han med at det er svært individuelt hva mennesker har tillit til. Fredrik mener at dette i seg selv er en utfordring for teknologisk fremgang som i utgangspunktet skal være tillitvekkende.

Fredriks synspunkt kan forklare hvorfor etikken rundt prediktive teknologier er omdiskutert i Norge. Fredriks tolkning er at dette handler om hvordan teknologien er utviklet i andre land og de etiske utfordringer som har dukket opp i den sammenheng. Denne tematikken vil diskuteres utover i avhandlingen. Anne snakker på sin side om hvordan dette ikke skal være et hinder for å utvikle og bruke slike verktøy. Dette begrunner hun med kravene som stilles til slik teknologi:

> «Vi stiller jo høyere krav til etikken innenfor KI enn vi stiller til etikken i det tradisjonelle arbeidet tror jeg nesten for å være helt ærlig. Men det skal jo også gjøres, fordi vi aksepterer bare feil og bias hos mennesker egentlig. Til sammenligning fra en maskin som skal gjøre det skikkelig og likt hver eneste gang.»

Anne mener at det foregår en kvalitetssikring av teknologier som skal implementeres i det norske samfunnet. Hun viser til at denne kvalitetssikringen er å anse som tryggere enn den som foregår ellers i tradisjonell og i mindre grad automatisert kriminalitetsforebygging, der det kun er mennesker som vurderer. Dette mener hun er på grunn av de strenge etiske retningslinjene som stilles til kunstig intelligens. Ifølge Vestby og Vestby (2019, s. 3) er det å holde politiet ansvarlig for egen praksis en nøkkelkomponent i demokratisk politiarbeid. En viktig del av dette er at politiet skal kunne gi forklaringer på sine faglige beslutninger og legitimere dem. Anvendelsen av prediktive programvarer eller automatiseringsprogramvarer har skapt en bekymring nettopp rundt politiets evne til å kunne redegjøre for sine beslutningsprosesser (Vestby & Vestby, 2019, s. 3). Dette skyldes at mange anser algoritmer som ugjennomsiktige i sin utforming og praktiske bruk. Vestby og Vestby (2019, s. 6) gjør i likhet med Anne en sammenligning mellom individet og teknologi; de forklarer dette med at maskinlæring til forskjell fra menneskelig beslutning er basert på kjente algoritmer. Når vi bruker teknologi kjenner vi til algoritmene, skriver dem ned i programmeringsspråk, og kan dermed kontrollere dataene. Dette kan gjøres gjennom eksempelvis å tilbakestille deres skjevheter fortløpende, mate spesielle treningsdata til modellen, eller stoppe læringsprosessen til enhver tid. Vestby og Vestby stiller derfor spørsmålstegn ved formeningen om at teknologien er ugjennomsiktig. De argumenterer for at maskiner på enkelte områder er mer gjennomsiktige enn menneskehjernen.

Videre mener Anne at det rettes mer fokus mot de problemstillinger som oppstår ved bruken av teknologi enn de problemstillinger som finnes i tradisjonelt forebyggende arbeid. Siden det i dag foregår en omfattende kvalitetssikring av teknologiers datagrunnlag, vil dette ifølge henne bidra til at teknologien også opptrer på riktig måte. Dette er i tråd med det Cato beskriver. Han mener at vi på den ene siden har pådrivere for forebyggende verktøy, mens vi på andre siden har aktører som ser de faktiske utfordringene ved utvikling og implementering av teknologi. Cato opplever at norske myndigheter er klar over disse utfordringene og at vi har en langsom utvikling av slike verktøy i Norge. Tilnærmingen hans er at Norge på bakgrunn av dette har et fornuftig forhold til forebyggende teknologi:

> «Så det er klart at det er mange drivere som drar i retning av å effektivisere ved bruk av teknologi. Teknologene er superhappy for det, politiet ønsker jo å få forebygge. Men så reises det en del av disse problemstillingene da som man kanskje... jeg opplever at norsk politi og ledelsen er bevisst på det her og det er sikkert derfor man ikke har kommet

> veldig langt i det også, men jeg tenker det er jo liksom drivere som gjør at man har lyst å gå i den retningen og jeg opplever at i Norge så har vi fornuftige forhold til det da.»

Også Bjørn som jobber mer praktisk rettet med å implementere slike verktøy, stiller seg på lik linje med de øvrige informantene. Bjørn forteller at hans mål er at de verktøyene som politiet bruker, skal være i orden når de settes «under lupen» for kontroll. Alle stegene i utviklingen av verktøy, må ifølge ham diskuteres underveis, slik at det ikke oppstår problemstillinger i etterkant av implementeringen. Bjørn mener at dersom det også vises til hvem som er beslutningstakere og til begrunnelsene deres, så vil en riktig bruk av teknologi være oppnåelig:

> «Ja, det tror jeg. Og det er jo det som er mitt mål da. Det som jeg har definert som et mål i min jobb er å gi verktøy til politiet som kan brukes og som, når noen begynner å se på det, ser at alt er i orden. Og det betyr at vi må være nøye når vi utvikler sant, ikke så fort. Og når vi ser på hvem politiet er i kontakt med så er det sånn og sånn. Derfor velger vi ut «de» og «de» når vi trener en modell. (...) det viktigste er at det er klart, og så er det nøye diskutert. Det er ikke bare sånt man finner ut etterpå. Det er en del av dokumentasjonen; hvem har bestemt det og hvorfor, med hvilken begrunnelse (...) Så jeg tror at det er mulig.»

Fellestrekket for informantene er at de snakker om verktøy som de mener konkret kan bidra til å forebygge ulike typer lovbrudd. Det handler dermed om å skape teknologiske dørstoppere for at kriminalitet ikke skal kunne finne sted. Innenfor kriminologien defineres dette som situasjonell kriminalitetsforebygging. En slik form for forebygging har utgangspunkt i individuelle risikofaktorer. Fokuset ligger på årsaksmekanismene i nåtid og er basert på tanken om at lovbrytere foretar rasjonelle valg. Hensikten er å påvirke de faktiske mulighetene for å begå kriminalitet, å vanskeliggjøre målene for kriminalitet, og å endre på situasjonen fremfor å endre individet som utfører handlingen. Slik forebygging vil derfor være situasjonsorientert. Utgangspunktet er å definere visse situasjoner som problematiske og vurdere hvordan vi best og mest hensiktsmessig kan iverksette tiltak (Clarke, 1995, s. 91). Bruken av forebyggende teknologi kan settes i sammenheng med en slik tilnærming til kriminalitet: Situasjonsbasert kriminalitetsforebygging åpner opp for målrettet kontroll, der hensikten er å identifisere og fjerne potensielle lovbrytere gjennom preventiv forebygging (Zedner, 2009, s. 88). Teknologi kan dermed brukes for å sikre samfunnet mot potensielle trusler.

Fredrik beskriver hvordan teknologien kan utføre oppgaver som mennesker ikke vil klare på egen hånd. Det vises til hvordan store mengder med chattelinjer ofte skal analyseres av politiet. Fredrik forklarer at de enorme mengdene informasjon er noe som mennesker selv ikke er i stand til å lese gjennom. Ifølge ham er dette en helt ulik prosess fra det vi ser på film hvor «du setter opp et bilde med en wipeover, og du plutselig har mistenkte der på to sekunder». Fredrik beskriver hvordan teknologi kan brukes til å gjenkjenne tekst på datamaskiner og sette ting i sammenheng. En form for automatisert prosess er derfor ifølge ham svært nyttig:

> «Det kan peke oss i retning av at «her bør vi se» også er det jo vi som tar beslutningen. Så det er ikke en sånn automatisering som du ser på sånne domstoler, at «her er du skyldig fordi AIen sa det». Det er ikke sånn det er, men det kan være en beslutningsstøtte og som et verktøy.»

Felles for informantenes uttalelser om en positiv bruk av forebyggende teknologi, er at de snakker om de teknologiske bruksområdene som i utgangspunktet finnes. Mulighetsrommet for en nyttig og god bruk av slike verktøy er i fokus. Informantene beskriver hvordan forebyggende teknologi kan brukes som en viktig beslutningsstøtte for politiet og hvordan det kan effektivisere tradisjonelt politiarbeid. Flertallet av informantene påpeker til tross for dette at en hurtig innføring av forebyggende teknologi ikke nødvendigvis er en riktig eller god måte å forebygge kriminalitet på. Ut ifra informantenes ståsted handler dette om at teknologien som implementeres skal være gjennomarbeidet, etterprøvbar og fri for feil og mangler. Slik kan teknologien bygge oppunder norske myndigheters samfunnstillit.

Jevnt over er det stort sett enighet og få nyanser å finne i de ulike informantenes narrativ om teknologioptimisme. Det som kan nevnes er at Bjørn, Anne, Gro og Dina snakker mye om hvordan teknologien kan plukke opp trender og utviklinger som i sin tur kan forebygge kriminalitet. De viser til at forebyggende verktøy kan bidra til å dekke opp behovene som finnes i politiet. De er dermed praktisk orienterte i sitt syn på forebyggende teknologi. De viser eksempelvis til forebygging ved bruk av nettverksanalyser, geografiske analyser, og bruken av bilde-, video- eller lydanalyse. Den praktiske samfunnsnytten til teknologi blir dermed tydelig vektlagt. Cato, Fredrik og Erik har i sine intervjuer et noe mer overordnet sikkerhetsfokus når de diskuterer teknologioptimisme. De viser til hvordan teknologi kan forebygge alvorlig kriminalitet. Lovbrudd som nevnes er menneskehandel, terrorisme og organisert narkotikakriminalitet. Erik mener eksempelvis at teknologien kan «være med på å trygge

befolkningen i det norske samfunnet». Halvparten er dermed mest opptatt av de forebyggende verktøy som teknologi kan skape, og den andre halvparten har fokus på de lovbrudd som kan forebygges og samfunnssikkerheten som teknologi kan gi. Samlet sett er dette dermed to ulike innfallsvinkler til teknologioptimisme. En mulig tolkning er at dette har sammenheng med informantenes kompetanse og yrkesrettede tilnærming til det aktuelle fagfeltet.

5.2.2 Teknologiens kompleksitet

Teknologi kan som beskrevet innledningsvis i kapittelet ha mye nytteverdi. Likevel kan teknologi fremme kompleksitet og sårbarhet. Ifølge Janet Chan (2021, s. 48) preges de sosiotekniske forestillingene om bruken av teknologi i politiarbeid av to motstridende utgangspunkt. I deler av politiet vises det til positive forestillinger, der teknologien kan bidra til økt effektivitet i arbeidet, tryggere lokalsamfunn og mindre kriminalitet. Visjoner rundt bruken av kunstig intelligens i politiet er «smartere politiarbeid». Chan (2021, s. 45) viser så til følgende: «AI, in spite of its widely circulated achievements, is not without problems». På andre siden finnes derfor de som stiller spørsmålstegn ved de uttalte fordelene, samt ved risikoen av å benytte KI i politiet. Et godt eksempel på hvordan disse motstridende holdningene spilles ut i praksis, er i det prediktive politiarbeidet. Debatten rundt dette viser til at det finnes en usikkerhet i teknologi og til hva teknologien kan predikere. Noen stiller spørsmål ved hvor sikker teknologi for kriminalitetsforebygging egentlig er. Andre viser også til svakheter ved hvordan teknologi kan forebygge lovbrudd (Chan, 2021, s. 48). De fleste informantene er opptatt av den iboende kompleksiteten til forebyggende teknologi. Hvordan teknologioptimisme og et teknologikritisk syn befinner seg i en symbiose viser en informant til ved følgende refleksjon:

> Anne: «Ja, jeg tror kanskje at noen av de største farene er fordi det råder en teknologioptimisme. (...) det er jo ofte litt enten eller, hvor noen er veldig pessimistiske og tenker at det her vil bare bli skjevt, feil og uetisk. Mens man i andre leiren kun ser på mulighetene vi har. Midt imellom tror jeg kanskje kjernen ligger. Kjernen handler ofte om hvilke problem det er vi faktisk har tenkt å løse. Hvis vi ikke tar oss tid til å starte der, så...»

Anne sier også at hun er redd for at teknologi «av og til kan virke som magi som skal hjelpe oss uten at en egentlig har satt foten i bakken og tenkt over disse tingene». Dette begrunner hun med en utbredt holdning preget av «enten-eller» til teknologi. Det første scenarioet beskriver

hun som total dystopi. Det andre scenarioet er voldsom optimisme og tanken om slutten på nettbasert kriminalitet så fort man får disse systemene på plass. Anne mener at vi i virkeligheten står i et spenn mellom disse to. Ifølge henne, handler det om å finne den balanserte holdningen hvor man tar teknologi «for det det er». Innenfor disse rammene mener hun at man må operere som politi, for ikke å bli for inngripende i folks frihet. Anne viser til at frihet er et viktig og krevende prinsipp innenfor teknologiutvikling. At det finnes en risiko for at teknologibruk kan være inngripende i menneskers frihet er noe flere av informantene tar opp. Dette er også en debatt som foregår både i Norge og utenfor Norges grenser. Samtidens frykt for de ulike implikasjonene av offentlig masseovervåkning er en sentral del av denne debatten, som allerede har pågått over lang tid (Ericson & Haggerty, 2000, s. 614).

Behovet for sikkerhet har resultert i at man identifiserer, klassifiserer og håndterer mistenkelige grupper i henhold til risikonivået de oppfattes å kunne utgjøre. Innenfor kriminologien betegnes dette som aktuarisme. Aktuarismen er en tilnærming til kriminalitetskontroll som vektlegger teknologi for risikominimering og -eliminering av potensielle trusler i samfunnet (Feeley & Simon, 1992, ss. 449-450). Dette erstatter dermed bakenforliggende forklaringer eller motiver bak lovbrudd. Konsekvensen er at teknologi både muliggjør og legitimerer forebyggende inngrep. Det å stole på risikovurderinger, forutsetter at trusler er kalkulerbare. Dette forutsetter også at mistenkelige populasjoner kan identifiseres upartisk i henhold til objektive kriterier og at de er basert på pålitelige data. Til tross for kravet om objektivitet, er det en utbredt skepsis til hvorvidt risikovurdering kan betraktes som en upolitisk og objektiv praksis (Zedner, 2009, s. 78). Bjørn snakker om tematikk som viser hvordan teknologi kan vanskeliggjøre en slik objektiv praksis:

> «Men det er mange problemer med det (...) det mest kjente eksempelet er fra USA hvor du trener en modell med bilder av alle de innsatte og så kan du kjenne igjen forbrytere ikke sant. Problemet er at det er en veldig stor sosial og rasemessig skjevhet i det grunnlaget og så får du modeller som er skjeve, som om har på en måte innebygde bias.»

At forebyggende teknologier kan inneholde elementer av skjevheter er noe flere av informantene snakker om i sine intervjuer. Dette støtter opp under forskning som viser til at ikke utelukkende kriminelle, men også enkeltpersoner og grupper som ikke er relatert til kriminell aktivitet, havner innunder overvåkningsverktøy eller blir utsatt for diskriminerende praksis (Niculescu-Dincă, 2021, s. 2). Likevel har det blitt hevdet at det ikke nødvendigvis er

teknologien i seg selv som er årsaken til dette, men at dette kan skyldes andre bakenforliggende faktorer. Det har også blitt påpekt at informasjonsteknologi kan spille en viktig rolle i å minimere de diskriminerende effektene av overvåkning, samt muliggjøre effektivt politiarbeid (Niculescu-Dincă, 2021, s. 2). På tross av dette er det i dag en utbredt motstand mot overvåkningsteknologier i en rekke fagmiljøer. Mye av dette handler om at moderne overvåkningsteknologi settes i sammenheng med ansiktsgjenkjenning. De diskriminerende aspekter som følge av dette anses som alvorlige og utbredte. Et eksempel er hvordan fargede personer og marginaliserte grupper i større grad fanges opp av slik teknologi (Radiya-Dixit, 2022). Dette vil diskuteres nærmere utover i avhandlingen.

Spennet i informantenes perspektiver på forebyggende teknologibruk, viser hvor kompleks tematikken rundt dette er. Det tydeliggjør også informantenes skepsis til teknologibruk i kriminalitetskontroll.

Flere av informantene beskriver hvordan utviklingen av forebyggende teknologi går langsomt i norsk politi i dag. Bjørn mener at det er en utfordring at teknologi som eksempelvis KI-verktøy ikke er tatt i bruk på en rekke felt. Ifølge ham er det en bølge av dette på vei, men det er likevel noe som ligger frem i tid. Bjørn viser til forebyggende teknologi som allerede brukes i andre land, og mener at det på en måte ville vært lettvint å kjøpe disse teknologiske løsningene og implementere dem i det norske samfunnet. På den andre siden er Bjørn tydelig på hvorfor dette ikke bør gjøres: «hvis noen begynner å stille spørsmål om hvordan han ble plukket ut og ikke hun... ja, fordi modellen er fra USA og det går ikke. Den typen ting må vi tenke på». Ifølge Bjørn er konsekvensen av dette at teknologiutviklingen i norsk politi går sakte. Dette er i tråd med det Gro snakker om; hun beskriver hvordan forutseende politiarbeid er et faglig krevende område som det er mye skepsis til. På tross av at nytten kan være stor, mener Gro at det kan ta tid før bruken av prediktive teknologier kan anvendes i praksis:

> «Så i forhold til forebyggende, så tror jeg at i Norge må det læres. Hvis man klarer å bli god på å lære av det som faktisk har skjedd og hvordan kriminalitetsutviklingen faktisk går, at vi først og fremst jobber med det så er det kanskje den veien å gå i forhold til å drive forebygging.»

Erik snakker om hvordan vi i Norge ønsker å ha kontroll når det kommer til bevegelser i det offentlige rom. Dette handler ifølge ham om å skulle trygge befolkningen. Erik viser også til at

den situasjonelle forebyggingen er den mest sentrale for politiet å benytte seg av i forbindelse med dette. I tillegg vil verktøy for å vurdere faren for gjentakelse eller mistenkelig atferd være en del av en slik forebyggende praksis. Erik mener at dette er en type utvikling som går fort. Det vises til at slike teknologier vil kunne gjenkjenne handlingsmønsteret til en person som går rundt i et område der det for eksempel er mye lommetyveri. Erik forklarer i likhet med Bjørn at man har kommet lengre med implementeringen av slike teknologier i andre land. Eriks tolkning er at det derfor kan være fristende å implementere og ta i bruk slike tekniske løsninger i Norge. Likevel påpeker han følgende:

> «Så er jo spørsmålet om man vil ha det sånn da. Og det er ganske gode grunner til at det ikke bør bli for mye av det slik at det blir et sånt overvåkningssamfunn eller det her trykket blir for sterkt i alle kanaler. Så noen må gjøre en helhetlig vurdering av det her, og av hvilke typer som oppleves som inngripende og så videre.»

Informantene viser til et mulighetsrom rundt den sikkerheten det er mulig å skape, men som potensielt kan gå på bekostning av andre viktige aspekter i samfunnet. Dette vannskillet er ifølge informantene krevende og vil utspille seg ulikt alt etter hvordan det norske samfunnet tar i bruk teknologier i forebyggende øyemed. Dette er en global utvikling som allerede går raskt. Forskning viser til at politi- og påtaletjenestene må forholde seg til denne utviklingen (Klepper, et al., 2021, s. 25). Et sentralt spørsmål er hvilken rolle politimyndigheter bør spille i denne sammenhengen. Det vises til at hvis politi- og påtaletjenestene skal ivareta rollen som forebygger i det teknologiske domenet, må den teknologiske kompetansen være på høyde med deres oppdrag. Samtidig vil det være en frykt i befolkningen for kreativ (mis-)bruk av teknologi i politi- og påtaletjenestene (Klepper, et al., 2021, s. 25). På bakgrunn av dette kan det fremmes en rekke kritiske spørsmål om grad av etisk bevissthet og kompetanse i politiet. Dette gjelder både i utviklingen av teknologi, samt i bruken av den.

5.2.3 Et kritisk syn på teknologi

En digital infrastruktur blir av mange knyttet til store endringer i politiets organisering. Samtidig innebærer og muliggjør slike løsninger i økende grad at offentlige og private aktører samarbeider om sikkerhet. Dette gjelder både nasjonalt og internasjonalt, samt lokalt og regionalt. Samtidig anses overvåkning for å være en nøkkelpraksis i moderne tilnærminger til politiarbeid (Klepper, et al., 2021, s. 2). Overvåkning defineres som en form for innsamling av informasjon. Ulike metoder benyttes i dag for å drive frem en slik innsamling (Fyfe, Gundhus,

& Rønn, 2018, s. 84). Overvåkning anses som en av de viktigste institusjonelle komponentene i senmoderniteten (Ericson & Haggerty, 2000, s. 606), og medfører i sin tur en rekke kritiske aspekter som vil diskuteres utover i avhandlingen. Et stort diskusjonstema er derfor om forebyggende teknologibruk i det hele tatt kan være noe man har tillit til. Dette har vært interessant å se hvordan informantene har stilt seg til.

Ingen av informantene er utelukkende negative til bruken av forebyggende teknologi. Dette er trolig naturlig siden alle informantene jobber innenfor dette fagfeltet. De er derimot svært opptatt av at teknologien skal utvikles, implementeres og brukes riktig. Hvordan intervjudeltakerne mener at dette kan gjøres vil diskuteres nærmere utover i avhandlingen. Flere av informantene trekker frem informasjonsutvekslingsprogrammet Palantir som eksempel på forebyggende teknologi i intervjuene sine. De stiller seg i den sammenhengen kritiske til flere aspekter rundt innføringen av dataprogrammet.

I 2016 begynte norsk politi arbeidet med det såkalte Prüm/Omnia-prosjektet som skulle sikre mer effektiv informasjonsutveksling mellom norsk politi og andre staters politimyndigheter. Leverandøren av en slik informasjonsutveksling var Palantir; et Silicon Valley-eid IT-selskap som spesialiserer seg på datanalyse og overvåkning. Palantir omtales om et moderne verktøy for stordataanlyse (Jørgensund, 2017). Deres forretningsmodell er å inngå avtaler med statlige kunder der de selger og implementerer programvare for sammenstilt og analysert informasjon. Senere samme året inngikk politiet en kontrakt med Palantir, der hensikten var å koble sammen data fra politiets ulike registrere for blant annet fingeravtrykk, DNA-profiler og informasjon om kjøretøy og førerkort. De ulike registrene skulle gjøres søkbare både nasjonalt og internasjonalt. Politiet kunne da lete etter koblinger mellom spor, finne sammenhenger mellom kriminalsaker og løse dem raskere. Programvaren som skulle sørge for dette het «Gotham», og ble i Norge omdøpt til Omnia. I 2019 kom det frem at kostandene var blitt større enn antatt og at prosjektet var kraftig forsinket. Dette på tross av at innkjøpet av programvaren har blitt omtalt som et viktig ledd «i kampen mot organisert og alvorlig kriminalitet og terror». Fagmiljøer hos Kripos rettet samtidig sterk kritikk mot Politidirektoratets prosjektstyring og målsetting for prosjektet. Tidligere leder av Justiskomiteen Lene Vågslid uttalte i etterkant følgende: «Det kan se ut til at summen på 100 millioner er brukt på et prosjekt som foreløpig ikke har gitt noen resultater» (Røyse, 2020).

Kritikere av Palantir har uttrykt bekymring for masseovervåkning av uskyldige (Grut, 2021). Bruken av verktøyet har av borgerrettsorganisasjoner blitt kalt for et «potensielt totalitært mareritt» (Stanley, 2011). En politiansatt har også uttalt at politiet har sett seg blinde på teknologiske muligheter og dermed glemt personvernet i møte med Palantir (Grut, 2021). Cato sier følgende når han snakker om implementeringen av teknologi for forebygging i Norge:

> «Men så er det en del områder hvor det er problematisk også. Og der må man liksom gå opp hele det sporet. Jeg opplever at i Norge så har vi fornuftige forhold til det da. Men samtidig så er det noen som pusher på at man skal komme seg videre. Du har sikkert lest om det; denne Palantir-programvaren som norsk politi kjøpte inn. De brukte mange titalls-hundretalls millioner på å kjøpe det inn. Også har man ikke gjort godt nok forarbeid, også ble det jo satt på bremsen (...).»

Cato beskriver her hvordan ønsket om å implementere Palantir førte til oppkjøp fra norsk politi uten at de nødvendige kontrollmekanismene ble foretatt. Mangelen på dette medfører ifølge Cato at man potensielt kan bli sittende på teknologiske løsninger som anses som problematiske. Både datagrunnlag og vanskeligheter med sammenkoblingen av data fra ulike kilder er eksempler på denne problematikken. Der Cato beskriver utfordringene med forarbeidet rundt Palantir, snakker Fredrik på sin side om andre kritiske aspekter ved Palantir. Ifølge ham kan det oppstå nye problemstillinger når et selskap skal lage tjenestesystemer for norske myndigheter. Fredrik forteller at når man baserer seg på et privat selskap, vil det oppstå utfordringer hvis eksempelvis selskapet går konkurs. Det stilles samtidig spørsmålstegn ved hvor man da skal få tak i ny kompetanse fortløpende. Fredrik trekker også frem utfordringer rundt personvern. Dette mener han at kan være vanskelig å ivareta på en god nok måte når private selskap skal håndtere sensitive data om den norske befolkningen.

Denne tematikken går Dina går nærmere inn på. Hun mener at hensikten bak Palantir kan være nyttig, men at det virker på henne som at selskapet samler inn alt av informasjon om innbyggere. Dette mener hun er problematisk og at det vil stride mot personvernet i Norge. Det stilles også spørsmålstegn ved hva Palantir faktisk gjør med all informasjonen de sitter på. Dina lufter samtidig bekymring rundt hva som vil skje dersom informasjonen brukes på feil måte og til politiske interesser. Teknologioptimisme kommer altså med viktige forutsetninger for informantene. Flere av intervjudeltakerne snakker om teknologienes negative implikasjoner dersom teknologien ikke er gjennomtenkt og gjennomarbeidet nok. Norske myndigheter ønsker

naturligvis å skape et trygt og godt samfunn, der lovbrudd forebygges effektivt og på best mulig måte. Anne viser til at et slikt ønske kan få konsekvenser for teknologiutviklingen:

> «(...) jeg har snakket om politikraften og det som gjelder styreblikket vårt. At (...) teknologioptimismen preges av litt for raske beslutninger noen ganger og man kan ha litt for overdreven tro på at dette vil løse et problem, også glemmer man å definere hva problemet man egentlig skal løse er. Man kan skape nye problemer ved å forsterke problemer uten å egentlig være klar over det. Så det å styre patruljer til et område er en kjent problemstilling hvis man bruker kunstig intelligens til å predikere hvor det skal skje. Også styres patruljene dit og er i stand til å se hva som helst, også fører det til uro. Det blir en selvforsterkende effekt av å styres rundt på grunnlag av data. Så det er mange etiske utfordringer, både store og små.»

Anne beskriver i dette sitatet et viktig poeng: for det første viser hun til at det som blikket vårt er rettet mot, også er det som teknologien rettes mot. Kriminologisk teori viser til at det overvåkende blikket på mange måter har forhåndsbestemt hvem og hva som skal utsettes for kontroll. Dette gjøres følgelig på bakgrunn av kategorisk mistanke, fremfor mistanke på bakgrunn av oppførsel. I de fleste samfunn er visse befolkningsgrupper diskursivt konstruert som sosiale problemer, kriminalisert og utsatt for et utpreget politiblikk (Hunt, et al., 2020, s. 4). Dette forekommer også i vestlige land, der innvandrere og etniske minoriteter lettere havner i politiets søkelys enn øvrige grupper (Fassin, 2013, referert i Saarikkomäki, et al., 2020, s. 4). Teknologi skaper dermed en dikotomi mellom rettferdighet og urettferdighet (Aas, Gundhus, & Lomell, 2009, s. 10). Et nytt spørsmål som da dukker opp, er «sikkerhet for hvem?». Hvem sin sikkerhet ønsker vi faktisk å ivareta gjennom kriminalitetsforebygging? Anne viser med andre ord til at bruken av prediktiv teknologi også kan være en reproduksjon av de forutinntatte holdninger som allerede finnes i samfunnet. Dette mener hun at kan være svært problematisk.

Nina Sunde (2022, s. 2) introduserer begrepet «teknologi-fallgruver». Dette handler om troen på at teknologien er nøytral, at fakta snakker for seg selv og antagelsen om feilfrie systemer. Denne typen holdninger kan knyttes til ideen om en «mekanisk objektivitet». Sunde (2022, s. 2) beskriver at en slik tro på objektivitet tar utgangspunkt i at maskiner produserer rikere, bedre og riktigere bevis enn mennesker er kapable til. Sunde viser til at slik tillit kommer til syne i lovverk eksempelvis i England og Wales: «in the absence of evidence to the contrary, the courts will presume that mechanical instruments were in order at the material time». Regelen som

regulerer tillatte elektroniske bevis, angir her en presumsjon om at datasystemer er pålitelige. Det er dermed viktig å merke seg at felles for flere av informantene, er deres synspunkt om at dagens datasystemer ikke nødvendigvis er pålitelige.

Fredrik drøfter hvorvidt han tror det er mulig å skape en tillitsfull bruk av teknologier for kriminalitetsforebygging. Fredriks tolkning er at det går an å skape en usynlig bruk av det, og at vi i fremtiden ikke engang vil reflektere over eller være klar over at det er teknologi som er rundt oss. Frederik viser til at det først er når du vet at noe er teknologi, at du tar stilling til om du har tillit til teknologien eller ikke. Fredrik trekker frem bruken av kunstig intelligens og eksemplifiserer:

> «Den klassiske at du chatter med noen du ikke er klar over at ikke er et menneske, og som egentlig er en maskin. Men jeg tror at mange nivåer av KI kan man spare seg for mye rot med hvis man bare ikke signaliserer at det her er det KI.. (...) det vil jo være individuelt da. Det vil være noen som ikke engang har tillit til 5G-nett engang, så det vil jo være et veldig stort spekter av hva folk har tillit til. Men jeg tror du helt fint kan implementere det uten at folk skjønner at det er KI inne i bildet. Så er spørsmålet om det er etisk riktig da, men det blir jo en annen diskusjon.»

Fritt leide for teknologibruk vil være en mulig følge av en slik usynlig implementering. Dette kan resultere i manglende oppmerksomhet rundt kvalitetssikring av den teknologien som skal benyttes for forebygging. Informantene viser til at det i Norge gjøres gode etiske vurderinger rundt det som skapes og implementeres. Dette er ikke nødvendigvis tilfelle i andre land. Hvem vil kunne stille spørsmål ved teknologi i forebyggende øyemed, dersom man ikke er klar over at kriminalitetskontrollen faktisk styres av teknologien? En slik utvikling vil potensielt kunne gi store konsekvenser i det norske samfunnet. David Lyon (2001, s. 23) skrev allerede for over 20 år siden at teknologi og samfunn er sammenbundet i en konstruksjonsprosess. Dette kan i aller høyeste grad være tilfellet i dag. Lyon mener at uavhengig av om det gjelder gatekameraer, innhentingen av persondata via internett, genetisk og biometrisk overvåkning eller annen teknologi, så vil teknologiene være uløselig knyttet til nettverk. Slike nettverk vil inkludere menneskelige aktører, sosiale organisasjoner og strukturer. Lyon mener at disse nettverkene vil operere etter koder knyttet til ulike menneskelige oppfatninger og ulike måter å håndtere risiko på. Dette betyr i praksis at det opereres med koder som ikke er nøytrale. Lyon mener at dette gjør nettverkene sårbare for etisk og politisk kritikk. I en mobil verden som utvikles raskt og

hvor mesteparten av de sosiale interaksjonene våre blir mer abstrakte, kreves det at overvåkningen i samfunnet holder følge. Nye teknologier opererer etter dette formålet og vil som konsekvens drive en umerkelig sosial klassifisering. Resultatet av dette er at det skapes en sosial orden (Lyon, 2001, ss. 26-27). En slik sosial orden er ikke nødvendigvis i tråd med de prinsipper Norge står for.

Informantenes perspektiver og Lyons argumentasjon synliggjør teknologiens kritiske aspekter. Lyon (2007, s. 40) beskriver hvordan politioppgaver i økende grad assosieres med kontroll, risiko og algoritmiske arbeidsmetoder. Lyon mener at en slik arbeidsmodell preges av foregripende aktiviteter. Det finnes flere bøker og filmer innen popularitetskulturen som tar utgangspunkt i en slik teknologisk utvikling. Et mye brukt eksempel i faglitteraturen er filmen «Minority Report». Her drives forebyggingen gjennom å gripe inn i lovbruddene *før* de forekommer (Lyon, 2007, s. 40). På mange måter gjenspeiler dette pre-kriminaliteten som er introdusert i kapittel 2 i avhandlingen. Lyon (2007, s. 139) mener samtidig at et slikt etablert fremtidssyn er preget av dystopi. Det vises til en dyster fremtid der sosial orden opprettholdes gjennom konstant overvåkning fra myndigheter. Han peker også på at dette er et fremtidig samfunn vi ønsker å unngå. Informantenes refleksjoner er ikke i tråd med en slik tankegang, men de er likevel opptatt av de mulige følger en ukritisk teknologibruk vil kunne ha i det norske samfunnet. Et sentralt spørsmål er dermed hvor informantene mener at vi skal rette blikket for å kunne skape en tillitsfull teknologibruk for kriminalitetsforebygging.

5.3 Hvem skal vi se til?

I FFI-rapporten fra 2021 beskrives det hvordan politiet i fremtiden skal kunne benytte teknologi for å utføre sine samfunnstjenester, herunder å videreutvikle teknologisk kunnskap, forståelse og kompetanse. Det vises til at dette bør gjøres gjennom «arenaer for erfaringsutveksling med nasjonale og internasjonale aktører». Europol, INTERPOL, FN, EU og politi i andre land fremheves som eksempel på slike aktører (Klepper, et al., 2021, s. 12). At dette trekkes frem som en viktig målsetting politiet bør etterstrebe, gjør det interessant å undersøke hvilke land og aktører som informantene mener at vi bør se til. I intervjuene er det tydelig enighet i hvilke land en ikke bør la seg inspirere av; herunder Kina og USA. Dette er noe alle informantene uoppfordret selv nevner, før de beskriver en positiv teknologiutvikling i ulike land eller hos ulike aktører. I den sammenheng vil jeg diskutere forebyggende teknologiutvikling i Nederland, Storbritannia og EU.

5.3.1 Kina

Flere av informantene innleder sin argumentasjon med å snakke om hvilke land Norge ikke skal se til. Her er det helt tydelig Kina som går igjen hos informantene. Fredrik uttaler følgende:

> «Vi kan se til Kina, også kan vi la være å gjøre sånn som de gjør. Det hadde vært fint. Men Kina er jo ganske rå på KI, og de har jo også som mål å være flinke. Så jeg tror det blir dumt å ikke se til dem og se hva de holder på med, fordi det treffer oss på et vis uansett. Men jeg tror ikke vi skal se til Kina og bygge opp samfunnet slik de har gjort.»

Her beskriver Fredrik hvordan Kina bruker teknologi for kriminalitetsforebygging på en måte som ikke er i tråd med kriminalitetsforebygging i det norske politiet. Denne tematikken går Gro nærmere inn på:

> «Så, når du snakker om teknologi så har jeg jo sett mye til Kina på hvordan de gjør overgrep på sin befolkning. Hvis du skal se på dem som ligger langt foran oss, så ligger jo Kina der; men det er jo ikke sikkert at det bestandig er den riktige måten å implementere teknologien på da (...). Ta for eksempel overvåkningskamera i Kina da, du har kanskje lest det, men der finnes det jo studier som viser at de bruker overvåkning som gapestokk; som viser at hvis du går på rødt lys så blir du markert så stor skjerm med rødt. Og de bruker jo også scoringssystem, men de forfølger også muslimene og setter dem i interneringsleire. Det har vært opp i to millioner av dem nå av 13 millioner i nord-øst, som har fått.. det blir jo som et fengsel hvor de blir lært opp hvordan de skal oppføre seg. Så det er jo der hvor teknologien brukes ekstremt dårlig, for å segregere et helt folkeslag. Så det er jo et eksempel på hvordan man kan bruke teknologien veldig rått og brutalt, og hvor man kan se et digitalt diktatur.»

Det Gro beskriver som overgrep og forfølgelser av bestemte grupper, omhandler befolkningen i Xinjiang-regionen i Kina. 48 % av befolkningen der er uigurer, en minoritet med tyrkisk avstamming. Av kinesiske myndigheter blir uigurene og andre øvrige etniske minoriteter mistenkt og ansett for å ha såkalte ekstremistiske holdninger. Bakgrunnen for dette er deres religiøse levesett. Konsekvensen er at mange av disse menneskene blir plassert i såkalte «omskoleringsleirer». Amnesty viser til at det i dag holdes opp mot en million mennesker i slike leirer, noe som Kina i en årrekke har forsøkt å avvise eksistensen av. Rapporter har vist

til at menneskene i leirene blir utsatt for hjernevasking, vold, seksuelle overgrep og tortur (Amnesty International, 2020).

Både Fredrik og Gro er i sine uttalelser kritiske til Kinas bruk av teknologi for forebygging. En del av det informantene trekker frem, er Kinas bruk av scoringssystemer, der store kinesiske teknologiselskaper gjennom overvåkning samler inn informasjon om innbyggere (Almås, 2019). Byrne og Marx (2011, s. 21) viser til at kinesiske myndigheter har utviklet teknologi som bruker Kinas nasjonale identifikasjonsbaser og ansiktsgjenkjenningsprogramvarer for å identifisere personer. Dette gjøres gjennom bruken av videoovervåkning. I Kina forebygger man dermed ikke bare kriminalitet gjennom teknologi; en regulerer også uønsket atferd. Forebygging blir i denne sammenhengen brukt til å kontrollere befolkningen i alle deler av samfunnet. Kina skal i 2020 ha registrert 1,3 milliarder innbyggere med biometrisk informasjon. Denne biometriske informasjonen skal også være kombinert med store datamengder fra både offentlige og private kilder. Kinesiske teknologiselskaper jobber tett opp mot kinesiske myndigheter, og har vokst seg store innen ansiktsgjenkjenningsteknologi og kunstig intelligens (Iversen, 2019). Gro påpeker at Kina er «rå på kunstig intelligens», og mener på bakgrunn av dette at det er lurt å se til hva kinesiske myndigheter holder på med. I flere av intervjuene gis det altså uttrykk for at Kina er dyktige på teknologi som omhandler kunstig intelligens. Det å lære av andre land «på godt og på vondt», er noe flere av informantene nevner. Med dette mener informantene at norske myndigheter kan lære av å studere en negativ bruk av forebyggende teknologier, like mye som de kan lære av en positiv bruk.

Cato trekker i sitt intervju frem et eksempel på hvordan Kina sin anvendelse av kunstig intelligente teknologier kan slå feil ut:

> «Det er sånn som med kvinnen i Kina som plutselig fikk veldig mye bøter inn på telefonen sin fordi hun hadde gått på rødt lys. Det er jo ikke lov i Kina. Så da fikk hun veldig mange bøter for det, også skjønte hun ikke det, fordi hun gikk jo aldri på rødt. Kjenner du til det eksempelet? For da hadde hun jo egentlig ansiktet sitt på bussen på en plakat og ble registret hver gang bussen kjørte på rødt. Så det der er jo sånn klønete måte å bruke AI på, da har du ikke testet det godt nok. Også kan man også stille seg spørsmålet om man skal ha den graden av automatisering i samfunnet at man skal få bot for absolutt alt du gjør feil. For da kan det bli et veldig slitsomt samfunn å leve i, hvis du skal unngå å få bot. Hvis du står på et gangfelt og ingen biler er i nærheten, men du

> fremdeles må vente på grønn mann. Så sånt mister man jo med KI, for det er jo et datasystem og datasystem er jo ikke så veldig god på å vurdere etikk og vurdere situasjoner utenom akkurat det det er laget for.»

Cato beskriver hvordan forebyggende teknologi blir en så stor del av samfunnet, at teknologien blir styrende for hvordan samfunnsmedlemmene oppfører seg. Dette anser han som et problematisk aspekt ved overvåkning, og som vil medføre etiske problemstillinger. Cato viser til hvordan teknologien vil kunne påvirke graden av frihet befolkningen i et samfunn har. Forskning viser at Kina i dag benytter teknologi som gir muligheten til å spore og overvåke innbyggere i alle aspekter av livene deres (Taylor, 2017, s. 2). Dette er tematikk samtlige av informantene som nevner Kina tar opp i sine intervjuer. De viser til hvordan kriminalitetskontroll går over i sosial kontroll og atferdsregulering, forstått som alle de mekanismer og ressurser som medlemmer av samfunnet bruker for normoverenstemmelser, og som de forsøker å få andre til å rette seg etter (Chriss, 2012, s. 18). Det er altså enighet blant informantene om at det finnes en rekke problematiske aspekter ved en slik tilnærming til forebygging.

5.3.2 USA

> Erik: «Ikke USA... for å si det sånn.»

Også USA er et eksempel som gjentatte ganger i intervjuene blir nevnt i negativ sammenheng. Imens Kinas bruk av teknologier direkte omtales av informanter som et «digitalt diktatur», beskrives imidlertid teknologi fra USA som problematisk når det kommer til personvern og bias:

> Bjørn: «Det er veldig lett å se til USA fordi veldig mye at det som finnes er fra USA. Men der har de et forhold til privathet som ikke vi deler.»

USA kan sies å være sterkt påvirket av den økende sikkerhetstankegangen. Terrorangrepene som fant sted 11. september 2001 har resultert i at risikostyring har havnet i forgrunnen av kriminalitetskontrollen. I 2002 uttalte Bush-administrasjonen følgende: «the greater the threat, the greater is the risk of inaction» (Fyfe, Gundhus, & Rønn, 2018, s. 37). I dag finner vi en riskobasert holdning til også andre typer lovbrudd i USA, ikke utelukkende til terrorhandlinger.

Dette har vist seg å ha store konsekvenser i det amerikanske samfunnet og har ført til en debatt rundt hvordan sikkerhet bør etterstrebes (Byrne & Marx, 2011, s. 24). Samtidig har teknologien innovert kriminalitetsforebygging; metalldetektorer på skoler og offentlige steder, bagasjekontroller på flyplasser, ulike sikkerhetssystemer og overvåkning er eksempler på dette (Byrne & Marx, 2011, s. 21). Forskningslitteraturen avdekker at teknologiadopsjonen i USA går i et svært raskt tempo, grunnet betydelig økonomisk støtte av amerikanske føderale myndigheter (Byrne & Marx, 2011, s. 25). Flere av informantene peker på en slik utvikling i USA:

> Gro: «Hvordan algoritmene styrer USA er jo kanskje noe vi ikke skal tilstrebe i Europa. Selv om vi ser at det kommer nå (...). Jeg har studert politiet (NYPD) på Manhattan og lært veldig mye. Men de har jo lov til nesten alt sant. De lagrer alle kjøretøy til og fra broen på Manhattan, så de har jo fått bukt med organisert kriminalitet. Men i Norge så hadde de jo flippet helt ut med den tilnærmingen fordi det er jo ren overvåkning.»

Gro danner her et skille mellom hvordan politiet i USA og i Norge opererer. Både hun og Bjørn beskriver at USA benytter mer inngripende virkemidler for kriminalitetskontroll. Gro kaller amerikansk politi sin tilnærming til forebygging for «ren overvåkning» av befolkningen. Hvordan amerikansk politi har utvidede virkemidler for forebygging kommer til syne i deres praksis. USA er eksempelvis det landet i verden med flest overvåkingskamera i verden etter Kina (Hansen, 2019). I informantenes forestillinger om masseovervåkningen av USA, mener de at det finnes flere problematiske aspekter. Dette handler i hovedsak om hvem de mener faktisk blir plukket opp av et slikt inngripende system. Det beskrives i flere av intervjuene at bias er en kjent utfordring:

> Bjørn: «(...) også tar man det eksempelet i USA hvor det bare er fargede som plukkes ut til kontroll fordi de matcher profilen og så videre.»

Rasisme innen straffesystemet anses på mange måter som et «amerikansk problem» (Earle, Parmar, Phillips, & Smith, 2020, s. 435). Forskning og statistikk viser til store sosioøkonomiske forskjeller mellom amerikanere som kan knyttes til hudfarge (Hunt, et al., 2020, s. 5). USA er blant landene hvor det oftest blir fremhevet et konfliktfylt forhold mellom politi og etniske minoriteter. Prosessuell rettferdighet betegnes som borgeres oppfatning av å bli behandlet med tillit, respekt, rettferdighet og deltakelse i strafferettsprosessen. Ifølge forskere er det mer

sannsynlig at etniske minoriteter opplever forekomsten av prosessuell urettferdighet enn øvrige grupper (Hunt, et al., 2020, s. 4). Sosiale medier og bevegelser som «Black Lives Matter» har de siste årene ført til at synligheten av slik rasisme og strukturell eksklusjon har blitt tydeligere. Dette har ført til at saker som omhandler diskriminering og urettferdig behandling på bakgrunn av rase har blitt satt på dagsordenen. Det som likevel er viktig å påpeke er at denne formen for eksklusjon av minoriteter ifølge forskning også finner sted i nordiske land (Hunt, et al., 2020, s. 5). Kanskje er det derfor også viktig å snakke om denne problematikken som ikke bare et amerikansk problem, men som et generelt samfunnsmessig problem.

Digital teknologi og kunstig intelligens blir i økende grad diskutert i lys av en slik diskrimineringsdynamikk. Ansiktsgjenkjenning, stordata-analyser og algoritmer implementeres i økende grad i strafferettslige sfærer. Dette gjøres med formål om effektivisering og sikkerhet. Utfordringen med slik teknologi er at den har vist seg å reprodusere kodede former for rasisme. Siden en slik rasisme på mange måter usynliggjøres, vil dette være krevende å spore og vanskelig å ansvarliggjøre noen for (Earle, Parmar, Phillips, & Smith, 2020, s. 439). Bjørns tolkning er at forebygging ved bruk av teknologiske verktøy og kunstig intelligens må gjøres på en riktig og grundig måte. Han beskriver hvordan det norske samfunnet er bygd på tillit, og at det er med denne tilliten i bunn at norsk politi forholder seg til den teknologiske utviklingen. Han sammenligner med USA, der han mener at dette ikke er tilfellet:

> «Det er på en måte min viktigste misjon (...). Fordi vi må være ekstra nøye med de greiene her. Fordi vi kan ikke, sånn som i USA handle, for så å rygge tilbake etterpå og si at «dette var dumt». Det er jeg veldig glad for at man også lengre opp i hierarkiet mener at er så viktig. At det er bedre at vi ikke har det verktøyet på plass i år, enn at det blir saker i media om at det bare er utlendinger som blir stoppet i trafikken.»

Det som går igjen i intervjuene er hvordan USA kan brukes som et dårlig eksempel på implementering av kriminalitetsforebyggende teknologi. Dina påpeker i den forbindelse at; «men man kan lære mye av dårlige eksempler». I tillegg skal det nevnes at USA også i likhet med Kina, blir nevnt i en sammenheng hvor det vises til at det finnes interessante aspekter ved deres forebygging:

> Gro: «Men mye av det som er der er jo både godt og dårlig da, men de har jo gått fra å ha 3000 drap i året til å ligge på 300. Så det er jo noe de gjør som er bra da, sånn sett.

> Så jeg har sett ganske mye på hvordan de jobber med kriminalitet og bekjempelse av kriminalitet (...) På Manhattan er det jo kjempefarlig å gå til husransakelse hvis det er bråk. Det er noe av det farligste du gjør; så når du er på tur ut til en leilighet eller en gård så får politiet der gjennom teknologien på håndholdte enheter beskjed om det er et farlig hjem før de dukker opp, eller om det er en farlig oppgang. Så de blir forebygget før de dukker opp da.»

Gros tolkning av amerikansk politis teknologibruk er at den kan ha en positiv effekt på forebygging. Det vises til at teknologien som benyttes i forkant av husransakelser er en måte «å ivareta betjentene du sender ut». Ifølge Gro er dette et eksempel på hvordan de benytter innrapportert kriminalitet og hendelser til å kunne sikre politiet på en trygg måte. Hun trekker så linjer til Norge og mener at det her er behov for å trene mer på innovasjon i politiet. Gro eksemplifiserer behovet for en slik innovasjon ved å beskrive trianguleringsteknologi som politiet i USA benytter. Dette er ifølge henne teknologi som detekterer og posisjonerer skudd fra skytevåpen ved å bruke mobiltelefoner som sensorer. Gro forteller at det trianguleres hvor skuddet kommer fra og styrer kamera i nærheten mot den registrerte hendelsen. Dette gjør at politiet kan få god oversikt over en hendelse tilnærmet samtidig som den faktisk skjer. Dette er et godt eksempel på hvordan teknologi endrer tidsaspektet rundt politiets forebygging. Som beskrevet i kapittel 2, vises det til at forebyggingen i økende grad forflyttes til sanntid. Gro forteller at denne typen trianguleringsteknologi er noe en har sett på også i Norge og som politiet har et ønske om å implementere.

Dette er i tråd med det som er illustrert som det nye «politi-paradigmet»; her er utgangspunktet at politiets strategi, respons og arbeid skal bli kunnskapsbasert og bygget på analytisk arbeid. Målet er at politiet skal kunne respondere bedre og raskere på mulige trusler i samfunnet (Fyfe, Gundhus, & Rønn, 2018, s. 63). En slik utvikling finner vi også i øvrige land. Likevel kan det av informantenes intervjuer virke som at USA er det fremste eksempelet på kompleksiteten i kriminalitetsforebygging. Både de positive følgene, samt slagsidene ved bruken av prediktiv teknologi er helt tydelige i intervjudeltagernes refleksjoner.

5.3.3 Nederland:

Når det i intervjuene beskrives hvilke land informantene tenker at vi skal se til i forbindelse med forebyggende teknologier, er det nesten uten unntak enighet om ett land; Nederland:

> Anne: «Nederland har gjort en del arbeid som retter seg inn mot dette...»
>
> Gro: «(...) Og så blir jeg bestandig inspirert av Nederlands politi, som er veldig langt fremme i Europa på utrolig mye (...). Så det er veldig inspirerende, samtidig som vi ikke bare kan gå på dem hele tiden. Vi må jo være sikre på at vi klarer å bygge opp det og så får vi heller søke inspirasjon fra de som ligger foran oss.»
>
> Erik: «Jeg tenker at Nederland er veldig interessant teknologisk sett fordi de har hvert fall tillatt eksperimentering med den der type teknologi i mye større grad enn andre på en kontrollert måte, der man har forskning knyttet opp til det (...). Så Nederland teknologisk sett og de innovasjonsprosessene de har, er interessante.»

Det er viktig å legge til at Erik påpeker at ikke alt i Nederland er «rosenrødt» og at det ikke nødvendigvis er sånn at det er ønskelig med «nederlandske tilstander» i Norge. Han mener likevel at norske myndigheter bør se til Nederland og deres innovasjonsprosess. Eriks tolkning er at det er helt nødvendig å «følge med i timen» dersom en ønsker en god og fornuftig bruk av fremtidig teknologi.

Flere av informantene viser til at Nederland ligger langt fremme innen både teknologiutvikling og -implementering. Flere nevner konkrete prosjekter de har sett på, tatt del i eller innehar kunnskap om. Dina mener at det er interessant å se hvordan nederlandsk politi selv snakker om teknologi. Hun er også opptatt av de moralske aspekter politiet i Nederland har rundt sin egen utvikling; herunder hvorvidt moralske spørsmål blir veldig styrende for deres arbeid eller om dette havner i bakgrunnen i forebyggingen. Dina forklarer at det er viktig at vi ikke bare ser på noe som fungerer i Nederland og dermed konkluderer med at dette er noe som Norge umiddelbart bør implementere selv. Dette synspunktet er noe som flere av informantene vektlegger. Likevel mener Dina at man kan se til Nederland og undersøke om deres teknologier har en overførbarhet til norsk politi:

> «Også prøver jeg å si at: ok, men kan de tingene man har trukket konklusjoner om gjelde her også da? Så litt det samme med teknologi da; man kan absolutt inspireres og se hvordan de har løst ting. Og så se om det er lurt.»

Bruken av automatisk skiltgjenkjenning på biler; såkalt ANPR, er noe som flere av informantene trekker frem i sine intervjuer i forbindelse med Nederland. Dette er et verkøy som bruker optisk gjenkjenning av tegn på bilder for å lese kjøretøys registreringsskilt. Gjennom denne avlesningen får politiet frem data om kjøretøyet. Det vises til at ANPR-kameraer gir mulighet til å fange opp ettersøkte for lovbrudd (Trædal, 2016). Dette er teknologi som benyttes i Nederland og i en rekke andre land. Siden 2012 har også alle utrykningspatruljer i norsk politi hatt ANPR-enheter. Politiet viser til at det er en teknologistøtte som gjør at de kan arbeide mer målrettet og kunnskapsbasert (Inderhaug, 2016). Patruljer som benytter automatisk nummerplategjenkjenning, pågriper ifølge statistikk fem ganger så mange kriminelle som ordinære patruljer (Inderhaug, 2014). Slike tall avdekker hvordan teknologi er et ledd i politiets kriminalitetskontroll. I 2018 ble det bestemt at bruken av ANPR skulle utvides til alle politidistrikter i Norge. Både Anne, Bjørn og Dina snakker om denne formen for kunstig intelligent teknologi og nytten den gir norsk politi:

> Anne: «Veitrafikk med skiltgjenkjenning hvor man raskt kan detektere om noen sitter med mobil eller om det er en stjålet bil og så videre. Innenfor alt finnes det en intelligent anvendelse av teknologi.»

Det vises til at Nederland er et av landene som har satset mye ressurser på forbedringer av ANPR-teknologien. Dette tydeliggjør hvorfor informantene beskriver at Nederland er langt fremme teknologisk og innovativt. Samtidig har ANPR i Nederland havnet under kritikk og blitt kalt en «massive privacy violation» (NL Times, 2021). Dette skjedde etter at det ble avdekket at nederlandsk politi hadde begynt å utforske alternative måter å bruke teknologien på. Politiet benyttet seg blant annet av utvidet lagringstid av data. Systemene lagret skiltene til millioner av biler i hele fire uker i politiets sentrale database for etterforskning og rettsforfølgelse. I et forsøk på å spore personer mistenkt for alvorlige lovbrudd ble det også klart at politiet ønsket å bruke gjenkjennbare bilder av passasjer og sjåfører fra ANPR-kameraer.

I et forsøk på å møte kritikken og beskytte folks personvern, har nederlandsk politi forsøkt å innsnevre ANPR-overvåkningen. I stedet for å lagre all trafikkdata, velger de kun ut mistenkelig atferd basert på sanntidsalgoritmer som behandler flyktige datastrømmer. Med en slik tilnærming har politiet tatt sikte på å ta kriminelle «på fersk gjerning» samtidig som at de kan få utføre sine politioppgaver (Niculescu-Dincă, 2021, s. 79). Gjennom dette viser myndighetene

i Nederland at de ønsker å handle i tråd med etiske retningslinjer. Dette kan også illustrere hvorfor informantene fremhever Nederland som et viktig land å se til for implementering av forebyggende teknologi. Det er også et eksempel på at teknologibruk endrer tidsaspektet rundt forebygging, samtidig som det reduserer lagring av persondata. Gjennom bruken av ANPR kan politiet gripe inn i sanntid, samtidig som et potensielt lovbrudd finner sted. Dette er med på å synliggjøre hvordan forebyggingsbegrepet blir mer foregripende.

5.3.4 Storbritannia

Når det kommer til Storbritannia, har informantene en noe blandet oppfatning av tilnærmingen til forebyggende teknologi. Først og fremst trekker noen av informantene frem at Storbritannia er langt fremme, men også spesifikk teknologibruk blir beskrevet som inspirerende:

> Fredrik: «Så vidt jeg vet så bruker alltid England og Nederland å være ganske langt fremme på den her typen ting. Så det er kanskje de landene jeg ville sett til da.»

> Gro: «(...) jeg kan ikke si hvor dere bør gå.. men jeg kan jo si at jeg blir veldig inspirert av England som bruker litt, men ikke så mye. De har mye bra metodikker på spesielt videoanalyse.»

Erik er positiv til landets teknologiske utvikling, men poengterer samtidig at det er et helt annerledes samfunn enn Norge. Erik anerkjenner at overvåkningen i Storbritannia er omfattende og at dette har bydd på utfordringer. Likevel mener han at landets myndigheter har håndtert dette på en god måte. Eksempelet på dette er teknologi som omhandler ansiktsgjenkjenning:

> Erik: «Så har jeg vel også sansen for en del av det som foregår i Storbritannia.. det er klart at det er et annet samfunn med et annet folk med veldig mange flere kameraer. Så man kan si hva man vil om det, men de har hvert fall en prosess på høyt nivå rundt reguleringen av det. Og der man har hatt noen saker oppe som jo har blitt vurdert, sånn som ansiktsgjenkjenning og bruken av det i det offentlige rom og der har man jo loven som strider om den typen overvåkning. Så det er jo på en måte forbilledlig, at man på en måte forsøker å muliggjøre en del av de problemstillingene de har av moralsk karakter i politiet generelt og det med teknologi spesielt i mange politidistriktene. Så det

er litt en bevegelse i det terrenget som vi kanskje bør begynne å ta etter i Norge når vi begynner å utvikle teknologi.»

Erik beskriver altså kontroversielle tilfeller i Storbritannia hvor ansiktsgjenkjenning har vært benyttet. I en rapport av Minderoo Centre for Technology and Democracy (Radiya-Dixit, 2022, s. 6) vises det til flere konkrete saker der bruken av ansiktsgjenkjenningsteknologi har blitt brukt på en måte i strid med landets lovverk. Teknologien som rapporten beskriver, er «Facial recognition technology» (FRT). Dette er et digitalt verktøy som brukes til å utføre oppgaver på bilder eller videoer av menneskelige ansikter (Radiya-Dixit, 2022, s. 13). Av rapporten fremgår det at bruken i samtlige av sakene ikke oppfylte etiske og juridiske standarder for styring av ansiktsgjenkjenningsteknologi. Konsekvensen har vært at myndighetene i Storbritannia har lagt opp til ny lovgivning og forbud mot politiets bruk av slik teknologi. Den britiske komiteen for justis- og innenrikssaker har samtidig tatt til orde for et sterkere juridisk rammeverk rundt teknologi innen rettshåndhevelse. Også mangelen på en klar linje for ansvarlighet for misbruk eller feil av slike verktøy har blitt påpekt (Radiya-Dixit, 2022, s. 10).

For informanten Erik er det han omtaler som «teknologisk bevegelse i terrenget», noe som det norske samfunnet kan se til. Dette handler om å prøve ut teknologi for å ta tak i de kriminalitetsutfordringene som finnes, for deretter å gjøre en vurdering av dem. Erik legger til at en kombinasjon av innovasjon og refleksjon er noe som er viktig å få på plass i Norge.

I Storbritannia har den raske utviklingen av ny digital teknologi, overvåkningskamera, roboter, droner og andre avanserte former for kriminalitetsforebyggende teknologier allerede hatt stor innvirkning på dagens politiarbeid. Det anses som sannsynlig at menneskelige former for politi vil minke, og at automatiserte kontrollprosesser vil øke (Liebling, Maruna, & McAra, 2019, s. 789). Eksempelvis er satellittsporing blitt viktig i britisk strafferett. Dette har potensialet til å ha kontinuerlig elektronisk overvåkning av personer uansett hvor de er. Slike typer verktøy føyer seg inn i rekken av teknologiske initiativer for forebygging som britisk politi utforsker (Liebling, Maruna, & McAra, 2019, s. 784).

Heidi Mork Lomell (2005, s. 237) beskriver hvordan videoovervåkning har økt siden 1980-tallet. Digitalisert overvåkning benyttes i dag både innen kriminalitetskontroll og av sikkerhetsinstanser. Både offentlige og private virksomheter bruker videoovervåking som verktøy for kontroll. Bruken av overvåkning kan derfor resultere i nye avvikskategorier,

ekskludering og frasortering i samfunnet. En slik overdreven bruk av overvåkning er noe Cato trekker frem i intervjuet sitt når det er snakk om forebyggingspraksisen i Storbritannia:

> «Noe ganske annet er hvert fall min opplevelse som du for eksempel har i Kina, USA og til dels Storbritannia. Storbritannia er jo det landet med flest CCTV-overvåkningskamera i forhold til størrelse i verden».

Cato trekker her paralleller mellom overvåkningen som foregår i Storbritannia og overvåkningen i USA og Kina. Som Cato beskriver, er bruken av overvåkningskameraer en sentral del av sikkerhetspraksisen i Storbritannia. En utbredt bruk av avansert teknologi for CCTV, gjør at de etter USA og Kina er det landet med flest overvåkningskameraer per innbygger i verden (Hansen, 2019). I dag ser vi også at ansiktsgjenkjenning har fått plass i en slik bruk av overvåkningspraksis. På denne måten kobles bilder til identitet. Hvordan slik teknologi påvirker politiets muligheter for forebygging er dermed et sentralt poeng. I Storbritannia blir det i stadig økende grad utviklet og benyttet ulik teknologi for ansiktsgjenkjenning. FRT-teknologi har blitt trukket frem som eksempel tidligere i dette delkapittelet. Britisk politi har begrunnet bruken av FRT med å skulle bekjempe terrorisme og alvorlig kriminalitet. Likevel har det blitt hevdet at bruken av FRT har strukket seg ut over de nevnte formål (Radiya-Dixit, 2022, s. 20). En slik utstrakt bruk av overvåkning kan knyttes opp mot beskrivelser av samfunnsmessige endringer i sosial kontroll, hvor risiko og sikkerhet innehar en sentral rolle i kriminalitetsforebygging:

> Crime becomes a risk to be calculated (both by the offender and by the potential victim) or an accident to be avoided, rather than amoral aberration which needs to be specially explained (Garland 1996, 451).

5.3.5 EU

Som nevnt innledningsvis i dette delkapittelet viser FFI-rapporten til ulike arenaer for erfaringsutveksling i bruken av forebyggende teknologi. Politimyndigheter i andre land har hittil i avhandlingen vært diskutert. Her har det blitt vist til Kina, USA, Nederland og Storbritannia. En annen aktør som FFI-rapporten (Klepper, et al., 2021, s. 81) trekker frem, er EU. EU blir også nevnt i flere av intervjuene:

> Bjørn: « (...) Sånn at jeg tror at Europa og EU bør være vårt referansegrunnlag.»

> Cato: «Altså, jeg tenker jo at EU er vel.. ikke et land da. Men det er hvert fall en institusjon da, over nasjonalinstitusjonen som hvert fall er et fyrtårn vil jeg si, når det kommer til å ta i bruk teknologi på en personvernvennlig måte. Så jeg tenker hvert fall at EU er fyrtårnet innenfor det området. Og de kommer med så vidt jeg skjønner gode styringsdokumenter, strategier og sånne ting.»

Viktigheten av personvern blir av informantene fremhevet som svært viktig når forebyggende teknologi skal utvikles og implementeres i Norge. Informantene anser samtidig EU som «et fyrtårn» for regelverk rundt slik teknologisk utvikling. Også teknologiutvikling innad i EU snakker informantene positivt om. Eksempelvis kan vi lese på EU sine nettsider at deres tilnærming til kunstig intelligens bygger på «excellence and trust, aiming to boost research and industrial capacity while ensuring safety and fundamental rights» (European Commision, 2023). EU har utarbeidet et lovverk kalt General Data Protection Regulation (GDPR), som landene innad i EU skal følge. Dette ble vedtatt i 2018. Gjennom EØS er også Norge i dag underlagt GDPR. Utgangspunktet for regelverket er at enkeltpersoner skal ha visse rettigheter vedrørende informasjon som samles inn om dem. Innsamlingen av slik informasjon skal også kreve en eller annen form for samtykke (Dencik & Sanchez-Monedero, 2022, s. 5). EUs regelverk legger samtidig begrensninger på hva det norske samfunnet kan bruke teknologi for. Dette fører ifølge Dina til en såkalt «treghet i systemet». En slik treghet anser hun som positivt:

> «Så er det jo så klart personvern da, som alltid er det som trekkes frem som en veldig stor ting. Og så har jeg litt samme tilnærming til det; at ja, veldig viktig og så klart ikke noe vi skal kimse av. Men vi har veldig gode lovverk rundt personvern også, som gjør at hvis vi ikke kan utvikle og ha et bevisst forhold til hva disse metodene brukes til eller hvordan de bruker dataene.. hva vi har lov til å samle inn, at vi har personvernloven i EU. Den ligger jo som en føring på alt vi gjør, og det er den vi skal forholde oss til.»

Dina mener at det er viktig at EUs regelverk finnes. Dette begrunner hun med de gode juridiske vurderingene som ligger til grunn. Dina viser til hvordan GDPR krever gode løsninger på oppbevaring av data, hvordan dataene brukes, hvordan de behandles og hva som kan publiseres. På bakgrunn av dette mener Dina at personvernloven i EU fungerer som et nyttig verktøy.

Cato trekker i sitt intervju frem Entry/Exit-System (ESS) som et konkret eksempel på hvordan EU driver grensekontroll ved bruk av teknologi. Dette er et inn- og utreisesystem utarbeidet av EU. Det foregår ved elektronisk registrering av tidspunkt og sted for reiser over Schengen-samarbeidets yttergrenser. Registreringen gjelder for tredjelandsborgere med korttidsopphold på Schengen-territoriet. Det er et automatisert IT-system som i tillegg til reisedokumentopplysninger vil registrere biometriske kjennetegn som ansiktsbilde og fingeravtrykk. Dataene vil bli kontrollert ved senere inn- og utreiser. Systemet vil foreta automatiske beregninger av hvor lenge personen har oppholdt seg på Schengen-territoriet. Systemet vil også varsle medlemslandene om reisende ikke forlater Schengen-territoriet innen utløpet av lovlig oppholdstid (EU, u.å.).

Systemets hensikt er å effektivisere grensekontrollprosessen. Ved å automatisere denne prosessen skal man slippe fysisk pass-stempling. Entry/Exit-System (ESS) skal gjøre det enklere å spore reisende som bruker falske identiteter og pass. I tillegg skal ESS forebygge, spore og etterforske terrorforsøk og andre alvorlige former for lovbrudd. Dessuten vil medlemstatenes rettshåndhevende myndigheter ha anledning til å gjøre søk i systemet når vilkårene for det er oppfylt. Dette omtales som et sekundærformål (EU, u.å.). Vi kan dermed se hvordan slik teknologi gjør seg gjeldende innenfor kriminalitetsforebygging. Sorteringen av personer og grupper inn i kategorier av «ønskede» og «ikke ønskede» er en sentral del av moderne teknologi sine virkeområder. Transnasjonale informasjonssystemer for politimyndigheter anses som ideell for en slik bruk av teknologi (Lyon, 2001, s. 98).

ESS kontrollerer individer som ikke er EU-borgere og som reiser til et europeisk land med kortholdsopphold på opp til 90 dager. Hvis personen har blitt nektet adgang til et EU-land som benytter ESS, vil dette bli registrert av systemet. Dersom personen nekter å oppgi biometrisk informasjon, vil personen bli nektet adgang til alle europeiske land som benytter systemet. Cato forklarer at dette er teknologi som skal tas i bruk fortløpende. Systemet er en omfattende innhenting av opplysninger for de som kontrolleres. Når begrunnelsen for teknologien er å styrke og beskytte de ytre grensene til Schengen, samt å skulle vokte og øke sikkerheten til innbyggerne (Schengenvisa, u.å.), kan vi se hvordan sikkerhetsbegrepet kommer til anvendelse. Når det er spesifikt beskrevet at en viktig del av ESS er å forebygge terrorhandlinger og andre alvorlige lovbruddformer, ser vi hvordan kriminalitetsforebygging skaper et bakteppe for overvåkning og kontroll av bestemte grupper i verdenssamfunnet. Det å skulle forebygge ytre farer og trusler er i tråd med den stadig økende tankegangen om å beskytte grensene og «sine

egne» (Aas, 2014, ss. 533-534). Forebygging er på bakgrunn av en slik argumentasjon også en ekskluderende praksis. Cato forklarer viktigheten av at ESS etableres på en forsvarlig måte. Ifølge ham er det en rekke kvalitetskrav som må ligge til grunn for teknologien.

KI-baserte overvåkingsteknologier som ansiktsgjenkjenning, emosjonsgjenkjenning og annen biometrisk teknologi blir i økende grad introdusert av både offentlig og privat virksomhet rundt om i verden. Dette har resultert i at EU i 2021 publiserte et forslag til et nytt AI-regelverk (Barkane, 2022). Ingen av informantene snakker i sine intervju konkret om EUs forslag. Flere av intervjudeltakerne er likevel inne på tematikk som er relevant for dette. En del av begrunnelsen for det nye regelverket er å adressere kunstig intelligent teknologis opasitet, kompleksitet, skjevheter, grad av uforutsigbarhet og delvis autonom oppførsel (Council of the European Union, 2020, s. 5). Dette er noe som informantene beskriver viktigheten av i sine intervjuer.

Erik snakker i sitt intervju mer generelt om EU sine reguleringer. Han mener at på tross av at føringene som EU pålegger en rekke land er positive, kan det også være en utfordring for politiet som ønsker å maksimere samfunnsnytten ved bruken av forebyggende verktøy:

> «Når man får sånn ansiktsgjenkjenningsteknologi så er det jo kjempefristende å benytte det i ulike sammenhenger. Men så bør man kanskje ikke gjøre dette uten at det er reguleringer. Og da har man EU som er en pådriver på det i dag, på sine lovgivninger på feltet og som står i sterk kontrast til det for eksempel skjer i USA. Men heller ikke den er skrevet i stein og den har vært vanskelig for politiet også å forholde seg til fordi man tenker at den har vært alt for streng hvis man tenker på de feltene der samfunnsnytten er så stor at man bør få lov til å utfolde seg i større grad. Så det er igjen et forhandlingsspørsmål som vi får se hvordan går, og når det er sånne utviklingstendenser så er det viktig at man har en etisk refleksjon rundt det.»

En slik etisk refleksjon på tvers av land settes i sammenheng med endringer i hvordan politiet arbeider med sitt samfunnsoppdrag. Mye kriminologisk litteratur har tidligere fokusert på det politiet gjør innenfor nasjonale grenser (Aas, 2013, s. 164). I dag ser vi imidlertid en utvikling hvor det i økende grad drives transnasjonalt politiarbeid. Dette gjelder i stor grad det forebyggende arbeidet. Land seg imellom samarbeider om internasjonal sikkerhet. Vi kan dermed snakke om en ny global politikultur (Aas, 2013, s. 165). Som EUs

personvernlovgivning er et eksempel på, har det også kommet internasjonale arenaer for regulering av politiarbeid. Det er dermed ikke bare land seg imellom som samarbeider for å bekjempe kriminalitet; det finnes også internasjonale regelverk, som eksempelvis i EU, som legger føringer på hvordan forebygging skal gjøres på en demokratisk, juridisk og etisk riktig måte. Som avhandlingen hittil har vist, er dette en krevende øvelse. Å bruke teknologi for kriminalitetsforebygging er ifølge informantene også krevende; noe jeg vil utdype i neste delkapittel.

5.4 Utfordringer ved forebyggede teknologi

Avhandlingen har hittil avdekket at både norske og internasjonale myndigheter i økende grad benytter teknologi basert på kunstig intelligens og maskinlæring for å forhindre kriminalitet. Avhandlingen har samtidig vist at en slik teknologibruk ikke nødvendigvis vil regnes som problemfri. Et sentralt spørsmål er derfor hvilke diskurser informantene trekker veksler på når de beskriver ulike utfordringer ved teknologi som skal forebygge kriminalitet. I dette delkapittelet vil det dermed også være relevant å se nærmere på informantenes ulike forståelser av forebyggingsbegrepet. Dette vil jeg gjøre gjennom følgende temaer: «innsyn», «sikkerhet for hvem?», «etikk og bias i data», og «tillit».

5.4.1 Innsyn

På bakgrunn av intervjuene vises det til flere problematiske aspekter som omhandler innsyn i teknologier. Vi kan på ene siden snakke om manglende innsyn i arbeidet rundt teknologiimplementering. På andre siden kan vi snakke om manglende innsyn i algoritmene som brukes i teknologiske verktøy. Informantenes oppfatning er at det kan være vanskeligheter med innsyn begge steder. Teknologi har potensialet til å fremme håp om de positive effektene av åpenhet for samfunnsmessig og organisatorisk atferd. Utgangspunktet er dermed at teknologi, stordata og algoritmisk intelligens kan styrke forebygging. Likevel har det vist seg at konsekvensen kan være utilsiktede muligheter for strategisk informasjonstilsløring, hemmelighold og ugjennomsiktighet (Flyverbom, 2019, ss. 12-13). Automatiserte sorteringsmekanismer, som kunstig intelligens og algoritmer kan brukes til å identifisere viktige mønstre og informere om beslutninger som eksempelvis omhandler kriminell aktivitet (Flyverbom, 2019, s. 5). Skal teknologien benyttes i forebyggende øyemed, vil det ifølge Bjørn være problematisk hvis slik teknologi har manglende innsyn:

> «Ukjent teknologi og magi kan ikke skilles fra hverandre hvis ikke du kjenner teknologien. Noe høres jo ut som magi hvis du ikke har vært borte i det før.»

Bjørn mener at mangelen på innsyn både kan handle om hvordan teknologien er bygd opp, samt hvilke vurderinger som er gjort i utviklingen av den. Det kan ifølge ham også handle om hvordan teknologien faktisk fungerer i praksis. Dette er i tråd med forskning som viser til store mangler i teknologisk kunnskap og teknologiforståelse i politiet (Klepper, et al., 2021, s. 82). Dette vil ifølge flere av informantene også gjelde den øvrige befolkningen uten noen form for utgangspunkt for kompetanse på feltet. Bjørn omtaler det som «en ball som det er vanskelig å få tak på». Denne typen problematikk går igjen også i andre intervjuer:

> Cato: «Det å finne ut «okei, hvordan skal vi bruke det?» og ikke minst KI, det må jo bruke programvare og hvem har egentlig produsert den programvaren? Hvordan er algoritmene konfigurert? Hvordan får samfunnet innsyn i hvilke typer algoritmer som benyttes eller programvare og hvordan de behandler dataene? Og overlater du hele det ansvaret til en privat aktør som du har kjøpt inn en programvare av? Uten å selv stille strenge kvalitetskrav og ikke engang kan kontrollere det så er det jo kjempeproblematisk…»

Cato mener at mangelen på kontroll er svært problematisk. Ifølge ham bør samfunnet stille krav til hvordan denne typen systemer faktisk skal fungere. Cato påpeker så følgende: «men det er jo ikke så mange som har dyptgående kunnskap om det så...». Catos mener at slik teknologisk kunnskapsmangel gjør det vanskelig for et samfunn å stille krav til noe vi ikke har forståelse for. Eksempelvis har Palantir vært diskutert tidligere i avhandlingen. Inntrykket er at selv flere av informantene som sitter på relevant faglig kunnskap synes det er vanskelig å forstå teknologien bak Palantir. Dette er et inntrykk som også forskningslitteratur deler. Iliadis og Acker (2022, s. 334) beskriver Palantir som et av de mest hemmelighetsfulle overvåkningsselskapene globalt sett.

En utgitt metoderapport om Palantir (Østli Jakobsen, 2021) beskriver utfordringer med innsynsmurer hos Politidirektoratet. Bakgrunnen for det ønskede innsynet var å forstå hva Palantir som teknologi faktisk innebefattet. Journalistene bak rapporten opplevde gjentatte avslag i sine begjæringer om innsyn i arbeidet rundt Palantir. En del av kritikken mot Palantir har derfor omhandlet manglende innsyn i prosessene rundt innføring og bruk av teknologien.

Dina sier i sitt intervju at hun mener det er viktig «å undersøke hva teknologi faktisk gjør». Hvis det er en teknologi fra USA (slik Palantir er), mener hun at det er viktig å ha visshet om hva selskapet gjør med dataene; «Drives selskapet av private interesser? Hva skal de bruke det til? Skal de selge det videre til noen andre?». Dina viser til at private aktører ikke nødvendigvis gir innsyn i sine algoritmer i frykt for at øvrige aktører kan ta dem og lage sine egne program. Likevel vil konsekvensen av dette ifølge henne være at transparensen blir dårlig og at åpenheten rundt en teknologi blir mangelfull. Dina sier følgende: «Det hjelper ikke med politiske debatter om teknologi man ikke vet hva egentlig handler om». Viktigheten av innsyn er noe også andre informanter trekker frem:

> Erik: «Det handler jo mye om forhandlinger der man må ta publikum eller borgerne med på laget for å finne ut hva som er fornuftig kontrolltrykk og hva som er akseptabelt med tanke på innsyn. Så alle kommer ikke til å bli enig, men hvis man ikke snakker om det så finner man aldri ut av det. Så der er en type åpenhet som er veldig viktig tenker jeg, slik at man ikke roter seg inn i et paternalistisk spor.»

Flere av informantene har en oppfatning av at det kan være problematisk å kjøpe løsninger av andre land eller private aktører. De viser til at det kan virke som en enkel løsning fordi teknologien kan kjøpes helt ferdig. Likevel har flere av informantene gitt inntrykk av at en slik måte å implementere forebyggende teknologi på, kan være problematisk. Dina viser til at vi bør forsøke å unngå politiske og private interesser når det kommer til forebyggende teknologi. Hun påpeker at private interesser likevel ofte havner i forgrunnen i teknologiutvikling. Informantene tolker det altså dithen at private og politiske interesser, kombinert med mangelen på innsyn er en tydelig problematisk side ved kriminalitetsforebyggende teknologi. Dette er ikke bare en utfordring ved teknologi fra private aktører, men ved generell bruk av forebyggende teknologi:

> (…) Databases and algorithms that produce predictions are notoriously hard to examine for non-professionals, because they are technically advanced and complex. They are, after all, the result of a collaboration of programmers, researchers, police officers and technologies. Even for software programmers it is at a certain stage no longer comprehensible how algorithms combine enormous amounts of data over time. This further raises problems of accountability and transparency (Kaufman, Egbert, & Leese, 2018, s. 687).

Transparens er altså et omdiskutert tema innenfor teknologiutvikling. På tross av ønsket om åpenhet og innsyn rundt teknologiske verktøy, kan dette i praksis være vanskelig å oppnå i dag. Palantir er et godt eksempel på nettopp dette. Mangelen på gjennomsiktighet vil i sin tur kunne ha uheldige konsekvenser. Dette er utgangspunktet for videre diskusjon.

5.4.2 Sikkerhet for hvem?

Som beskrevet tidligere i avhandlingen har sikkerhetsperspektiver siden 1990-tallet og begynnelsen av 2000-tallet beveget seg inn i kriminalitetskontrollen. Dette gjelder både retorikk, fokusområder og arbeidsmetoder. Også i Norge har vi sett en tydelig utvikling i denne retningen. Dette har i sin tur medført at sikkerhetstankegangen har fått en sentral plass i måten politiet forebygger kriminalitet på (Kaufman, 2018, s. 22). Et viktig spørsmål er dermed hvor langt man skal strekke seg for sikkerheten og hvem i samfunnet vi egentlig skal sikre og skape trygghet for. Informantene er opptatt av grenser for politiets bruk av overvåkning i samfunnet. Cato beskriver dette nærmere ved følgende refleksjon:

> «La oss si at politiet har fått droner, bruker de dronene til å identifisere personer som du har en eller annen mistanke.. ikke nødvendigvis mistanke, men som du ønsker rett og slett å få identifisert fortløpende da, basert på en eller annen input. (...) nå kjenner ikke jeg området i detalj. Det kan jo tenkes at lovverket åpner for det i forbindelse med spesielle begivenheter, la oss si for eksempel en demonstrasjon. Så bruker du en sånn drone med ansiktsgjenkjenning også får du identifisert for eksempel personer man må være spesielt oppmerksom på, men i en helt vanlig situasjon i et helt normalt bybilde som det her, så ville det jo vært kjempeproblematisk å bruke en sånn type teknologi her sant. Det ville jo nærmest vært sånn de bruker det nå i Kina i forbindelse med Covid-13 for å holde kontroll på folk.»

Utsagnet til Cato trekker veksler på diskurser om at frykten for sikkerhetsfarer kan åpne opp for et inngripende lovverk, som for eksempel økt overvåking (Kaufman, 2018, ss. 22-23). I Norge er det i dag et strengt regulert lovverk vedrørende bruken av ansiktsgjenkjenningsteknologi til kontrollformål. Dette gjelder også til kriminalitetsforebyggende formål.[6] All behandling av personopplysninger må ha et rettslig

[6] Dette kommer frem av EUs regelverk om personvern; GDPR, som Norge forholder seg til i dag. Dette gjelder både for private og offentlige enheter (https://commission.europa.eu/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_en)

grunnlag for å være tillatt. Et rettslig grunnlag forutsetter et behandlingsgrunnlag. Så lenge dette ikke finnes vil ikke bruken av personopplysningene være lovlig (Datatilsynet, 2019). På tross av dette har det blitt avdekket at Kripos har utforsket teknologien Clearview. Dette er en app som samler inn bilder av ansikter gjennom Facebook, Instagram, nettsider og andre sosiale medier. Ved å søke på ett fotografi av en persons ansikt, vil Clearview kunne bruke den innsamlede dataen til å gjenkjenne personen og gi tilgang til offentlig tilgjengelig informasjon om vedkommende. Det har blitt vist til at databasen i Clearview er i strid med både norsk og europeisk personvernlov (Skille, 2020). Dette viser at teknologiutvikling og implementering er et krevende felt for politimyndigheter, der norsk politi må trå varsomt i henhold til gjeldende lovverk.

Storbritannias bruk av kameraovervåkning har vært diskutert tidligere i avhandlingen, og er dermed relevant å trekke frem som eksempel i denne sammenhengen: Britisk politi benytter i dag kunstig intelligens for ansiktsgjenkjenning som en del av deres overvåkningspraksis. I en rapport av Minderoo Centre for Technology and Democracy (Radiya-Dixit, 2022) beskrives det hvordan domstoler har ment at måten britisk politi har brukt slik ansiktsgjenkjenning på er et brudd på personvernrettigheter. Det finnes også bekymringer om rasemessig skjevhet ved bruk av slik teknologi. Rapporten vektlegger at politiets bruk av ansiktsgjenkjenning ikke klarer å inkludere mange av de kjente praksisene for sikker og etisk bruk av datasystemer i storskala. Det vises til at problemet omhandler både mulige skjevheter i algoritmene og potensielle brudd på menneskerettigheter (Dodd, 2022).

Britisk politi har forsvart bruken av teknologien ved å peke på ansiktsgjenkjenning som et middel for å identifisere sårbare, savnede og ettersøkte personer. Samtidig beskriver de verktøyet som et bidrag til å bekjempe kriminalitet og forhindre trusler mot offentlig sikkerhet (Radiya-Dixit, 2022, s. 10). Gjennom uttalelsene til britiske myndigheter kan vi dermed se hvordan sikkerhetstankegangen kommer til uttrykk gjennom kriminalitetskontrollen. Det er også tydelig at bruken av overvåkning og ansiktsgjenkjenning er omstridt, også i land hvor lovverket i større grad har åpnet opp for slik teknologi. Vi kan dermed både snakke om utfordringer som oppstår ved teknologibruk, og de skjevheter som allerede eksisterer og som forsterkes ved bruken av forebyggende teknologi. Dette er i tråd med Catos beskrivelser:

> «(...) Sånn som jeg ser det så er jo litt av utfordringen med forebygging, at du aldri har en fasit på hva som inntreffer i fremtiden, sånn at du bruker historiske data til å prøve å

> predikere noe fremover. Og de dataene de kan både være skjeve, basert på at politiet for eksempel har oppsøkt vedkommende mange ganger, de har ikke oppsøkt person b eller c veldig mye, men person a har de oppsøkt. Selv om person b eller c har gjort like mye ugagn.»

Cato trekker her veksler på kompleksiteten ved forebyggende teknologi. Ifølge ham kan teknologi være en kilde til diskriminering, der innsamlede data resulterer i såkalte «feedback loops». Dette betyr i praksis at bestemte personer vil treffes hyppigere av teknologiene. Derfor vil de også oftere havne innunder kriminalitetskontrollen (Chan, 2021, s. 53). Potensielle skjevheter i data er derfor ifølge ham en klar utfordring. Dette vil utdypes på et senere tidspunkt i avhandlingen. Cato fremmer samtidig et av de viktigste elementene ved det å skulle være i forkant av lovbrudd: Dette handler om at det er en svært krevende øvelse, som aldri vil kunne være helt presis. Cato beskriver hvordan forebyggende teknologi ikke vil kunne gjenspeile den faktiske virkeligheten. Når målet om et trygt samfunn preger måten myndighetene arbeider på, vil dette kunne ha utilsiktede konsekvenser. Prediktive analyser forespeiler en «målrettet styring», hvor sikkerhetsbeslutninger skal forhindre trusler mot samfunnet. Slike analyser går utover grensene for «det kjente», og skal avdekke «det ukjente» (McCulloch & Wilson, 2017, ss. 80-81). Riskobegrepet gir en antagelse av at man kan forutse fremtiden og gjøre noe med den. Likevel anses dette som en iboende spekulativ og usikker prosess. Dette vil også gjenspeiles i inngripen mot forestilte fremtidige hendelser. Å forespeile risiko skaper samtidig potensielt nye former for risiko. I strafferett er eksempler på dette strengere straffer, forebyggende forvaring og utvidet politimyndighet (McCulloch & Wilson, 2017, s. 37). Vi så i kapittel 2 at Stanley Cohens beskrivelser av et overvåkende og straffende samfunn medførte nye mønster for sosial kontroll og derav nye avvikskategorier. Catos utsagn belyser hvordan forebyggende teknologi ikke nødvendigvis alltid vil opptre etter sin opprinnelige hensikt.

Erik har en annen innfallsvinkel i sitt intervju. Han beskriver situasjoner hvor sikkerhet havner i forgrunnen for kriminalitetskontroll og teknologi dermed risikerer å bli udemokratisk:

> «Man ser jo for eksempel at når det kommer en krise, som for eksempel korona, så er man villig til å gi fra seg en del frihet for at samfunnet skal nå sine mål. Hvis det er en stor trussel fra en nabo for eksempel så må man også.. det er jo situasjonsbetinget sant, og et spørsmål om hvor lenge den varer. Og om det vil bølge frem og tilbake, og det er ikke engang sikkert at det kan bølge frem og

> tilbake fordi man allerede har sluppet ånden ut av flaska og det dermed er vanskelig å få den tilbake igjen. Så man skal nok ha en treghet i det systemet.»

Erik viser altså til viktigheten av det skal være en «treghet i systemet». Dette forklares med at det ikke kun skal være politiets ønsker og folkemeninger som skal tas hensyn til, men også et rettsvesen som sørger for at prosessene som omhandler teknologi males sakte. Erik mener at noe av problemet er at man har en lovgivning som er virksom lenge etter at det har blitt åpnet opp for den. Dette skaper ifølge ham en gråsone, der han mener at det kan opereres på en udemokratisk måte. Han eksemplifiserer med ansiktsgjenkjenningsteknologi og sier at det kan være svært fristende å benytte dette i ulike sammenhenger som er utenfor den egentlige tiltenkte hensikten. Han påpeker at dette derfor er noe som tydelig krever reguleringer.

I diskusjonen om bruken av teknologi innen kriminalitetsforebygging, trekker informantene på kritiske diskurser om overvåkning og faren for at moderne kriminalitetskontroll innføres på bekostning av borgerens frihet og rett til privatliv. Informantene trekker i sine intervjuer paralleller mellom slike kritiske diskurser og den økende sikkerhetstankegangen. Det gjør også Lucia Zedner (2009, s. 123); hun viser til at når sikkerhetsbegrepets språk havner inn under kriminalitetskontrollens mekanismer, åpner dette opp for en økt inngripen av staten med tilhørende sikkerhetstiltak utformet for å håndtere nødsituasjoner. Vi risikerer dermed at sikkerhetstiltak brukes langt ut over den antatte krisetid. En ytterligere konsekvens kan være at disse sikkerhetstiltakene blir permanente og normaliserte, og dermed blir en del av styringsmodellen og internert i den ordinære kriminalitetskontrollen. Teknologi som overvåkning, massedatainnsamling og identitetskontroller trekkes frem som eksempler på dette og er i dag er en del av den generelle kriminalitetsforebyggingen (Lyon, 2007, referert i Zedner, 2009, s. 125). Hvorvidt vi skal bytte frihet og retten til privatliv mot trygghet, er ifølge informantene ikke bare et spørsmål om rettslige dilemmaer, men også moralske.

Det finnes flere fellestrekk i informantenes intervjuer. De beskriver alle ulike scenarioer hvor det å forsøke å komme potensielle lovbrudd og lovbrytere i forkjøpet, blir så viktig at det kan gå på bekostning av viktige prinsipper i det norske samfunnet. Den konkrete teknologien informantene beskriver muliggjør å foregripe hendelser, fremfor å drive forebygging. Det kan trekkes tydelige paralleller mellom slike teknologier og pre-kriminalitet. Et nytt spørsmål som trenger svar, er hvilke grupper i samfunnet som må ta konsekvensene av dette.

5.4.3 Etikk og bias i data

Flertallet av informantene beskriver hvordan bestemte grupper risikerer å bli mer overvåket og utsatt for kontroll ved bruk av teknologi i forebyggende øyemed. Dette er en sentral diskurs i forskning på moralske aspekter, ved innføring av teknologier og foregripende kriminalitetskontroll:

> The integration of risks and security into the criminal justice system (…) has led to ever-more coercive measures being introduced to stop and disrupt crimes that have not yet occurred but are predicted to take place. This raises questions about the awareness and recognition of biases (Fyfe, Gundhus, & Rønn, 2018, s. 9).

En viktig problemstilling er hvordan lovgivningen skal forholde seg til hva som gir grunnlag for å foreta forebyggende overvåkning. Hvilke mennesker, grupper av mennesker eller aktiviteter skal anses som utløsende for en slik inngripen? Beslutningstakere er i dag på mange måter i stand til å foreta skjeve utvalg med såkalte «bias» basert på egne holdninger eller verdier. En kritikk av proaktive forebyggende strategier er at noen kategorier av mennesker som lett kan anses som mistenkelige, i større grad blir rettet oppmerksomhet mot enn øvrige grupper i samfunnet. Dette betyr i praksis at bestemte individer fra disse mistenkeliggjorte gruppene blir utsatt for mer omfattende overvåkning enn andre (Fyfe, Gundhus, & Rønn, 2018, s. 11). Mistanker kan også rettes mot personer som ikke gjør noe ulovlig i utgangspunktet. De vil i verste fall måtte ende opp med å forsvare sin uskyld på tross av dette (Fyfe, Gundhus, & Rønn, 2018, s. 97). Zedner og Ashworth (2014, s. 53) presenter det de kaller «the presumption of innocence». En slik uskyldpresumsjon handler om at enhver person har retten til å bli ansett som uskyldig inntil og med mindre siktet og dømt for lovbrudd. Utgangspunktet er at staten skal anta at individer er ufarlige, så lenge det ikke finnes svært viktige begrunnelser for noe annet. Kanskje kan det ut ifra informantenes intervjuer tolkes dithen at en slik uskyldpresumsjon i dag er svekket. Til tross for kravet om objektivitet, stilles det spørsmålstegn ved om risikovurdering faktisk kan betraktes som en upolitisk og objektivt vitenskapelig øvelse (Zedner, 2009, s. 78). Profilering av potensielle lovbrytere kan av sine kritikere sies å være like mye basert på institusjonelle og sosiopolitiske bestemte kategorier, som på vitenskapelige vurderinger av hvem som utgjør mest risiko (Zedner, 2009, s. 79).

Katja Franko (2013, s. 78) argumenterer for at representasjonen av kriminalitet og avvik er innebygd i sosiale samfunnsstrukturer. Disse representasjonene speiler de inkluderende og

ekskluderende forholdene i gitte samfunn. Franko viser dermed til eksisterende skjevheter som finnes i et samfunn. Chan (2021, s. 46) beskriver at slike iboende skjevheter også vil finnes i teknologi. Dette vil kunne komme fra teknologiske begrensinger i data, historiske skjevheter som stammer fra feilaktige data eller fra teknologer som utvikler teknologi og som har tilsiktede eller utilsiktede bias. Konsekvensen av dette er at teknologi vil opprettholde disse skjevhetene. Det vil også kunne føre til at forebyggende teknologi vil rette seg spesielt mot spesifikke personer med bestemte egenskaper. Et sentralt spørsmål er dermed hvordan informantene reflekterer over dette.

Dina forteller følgende om etiske perspektiver ved forebyggende teknologi:

> «Det finnes masse muligheter (...). Men så er det så klart sånn at der er mye utfordringer også; hvordan det bygges opp hvis det ikke gjøres på en god måte eller hvordan det kan tas i bruk og bli feil brukt. Så mye av det vi har vært inne på, angående politiske og private interesser, fraskrivelse av ansvar, bias som jo man kan si at alltid ligger i dataene... Det er det jo også hos oss, men man kan jo ikke bare si sånn «ja, men fordi det er hos begge så er det greit». Men der er jo likevel sånne utfordringer da, og at man ofte implementerer det litt for raskt og da får veldig mye etiske utfordringer.»

Dina viser i likhet med forskningslitteraturen til de eksisterende skjevhetene som finnes i dataene, og som slik vil komme til uttrykk i teknologien. Også Bjørn beskriver hvordan man gjennom forebyggende teknologi risikerer å rette oppmerksomheten og mistanken mot bestemte personer eller steder, som følge av innebygde bias:

> «Vi kan ikke bruke data fra hvor ting har skjedd for å gi politiet råd om hvor de bør være til stede. Årsaken til det er som følger: hvis det står en bil på Stovner og det ikke står en bil på Frogner. Hvis to ungdommer begynner og sloss, så blir det ikke oppdaget av politiet på Frogner, men det blir oppdaget på Stovner fordi det står en bil der. Også kommer det opp at «okei, det er slåsskamp mellom ungdommer på Stovner». Og da blir det enda flere biler på Stovner, men kriminaliteten utvikler seg kanskje på Frogner, men det er det ingen som ser. Og da blir rådet til politiet å være mer på Stovner. Ikke sant? Og det er et velkjent eksempel som veldig ofte tas frem som et eksempel på hvorfor.. altså det kan være veldig fristende å lete etter skjulte trender i gamle data, men det er skumle greier fordi det som har skjedd reflekterer hva politiet tenkte og hvor politiet var

> da. Fordi at en slåsskamp er ikke en slåsskamp. En slåsskamp som politiet ser, er noe annet enn en slåsskamp som politiet ikke ser. Ikke sant?»

Bjørn viser til at dette er et typisk eksempel på noe som må unngås i forebyggende arbeid. Ifølge ham er dette et viktig etisk dilemma knyttet til bruken av data. Bjørn stiller spørsmålstegn ved hvor synlig slike skjevheter egentlig er, og sier følgende: «For greier vi å se innebygde bias; altså data som tilsynelatende er nøytrale, men som egentlig ikke er det?». Ifølge Bjørn er realiteten at input-dataene i teknologiske løsninger sjeldent er representative, og at dette skyldes en rekke ulike «bias-er» som ligger til grunn. Bjørns tolkning er i tråd med sosialkonstruktivistiske perspektiver: Powell, Stratton og Cameron (2018, ss. 122-123) viser til at koder og algoritmer ikke er nøytrale i utgangspunktet. Ved siden av programvaren og maskinvaren er det på hvert nivå av teknologien en grad av menneskelig input som vil ha påvirkning på teknologien. Slike menneskelige inputs vil gjenspeile programmererens kjønn, etnisitet, kultur, kunnskap og verdier. Også ytre faktorer som økonomiske, politiske og samfunnsmessige aspekter vil kunne ha en påvirkning.

Videre sier Bjørn at:

> «Men det er mange problemer med det her (...) det mest kjente eksempelet er fra USA hvor du trener en modell med bilder av alle de innsatte også kan du kjenne igjen forbrytere ikke sant. Problemet er at det er en veldig stor sosial og rasemessig skjevhet i det grunnlaget også da får du modeller som er på en måte skjeve. Som på en måte har innebygde bias, som er ordet vi bruker. Så vi kan ikke uten videre kjøpe ting, vi må ofte lage ting selv for å kunne dokumentere at her har vi tenkt på det greiene her, det er tatt vare på dette og dette.»

En åpenhet om de biaser teknologier fører med seg blir ansett som viktig av informantene. Dette støttes opp av forskningslitteratur: Gundhus (Fyfe, Gundhus, & Rønn, 2018, s. 240) peker på at risikoanalyser innenfor kriminalitetskontroll aldri vil være nøytrale. Vi må derfor se risiko i lys av innebygde skjevheter. Gundhus viser til at en eksplisitt diskusjon og bevissthet om disse skjevhetene til en viss grad kan bidra til å redusere dem.

Bjørn skiller seg likevel fra de andre informantene ved å fremholde at det er viktig å ikke bli for opphengt i problemstillinger rundt bias. Bjørn peker på at det finnes en fare ved å gjøre dette:

> «Nå driver (...) og lager en løsning som plukker ut navn i tekst. Det kan brukes både til hvitvasking og til å lete etter interessante personer i samtalegrupper, hos personer som for eksempel begynner å snakke om statsministeren sant. Da blir (...) bekymret sant, og tenker hvorfor gjør du det? Så den teknologien å lete etter navn i tekst kan brukes i mange forskjellige sammenhenger. Og igjen da, det som da er viktig er å si at (...) for eksempel ikke bare finner norske navn og ingen utenlandske. Sånn at de med utenlandske navn, at ingen av dem blir plukket opp. Eller at bare de blir plukket opp, ikke sant. At heter du Muhammed så havner du i klisteret med en gang. Det å kunne dokumentere at det har (...) tenkt på og det har blitt tatt hensyn til, men også å forklare hvordan det er sånn at den ene typen navn blir lettere plukket opp og hva som gjør det.»

Bjørn vektlegger at politiet må kunne dokumentere at de har tenkt på ulike problemstillinger som kan dukke opp i teknologiutvikling. Ifølge ham er det viktig å fremlegge informasjon som viser at disse problemstillingene er blitt tatt hensyn til. Bjørn mener også at datamodeller må trenes med korrekte og reelle data. Videre gir han et eksempel på dette:

> «Er det sånn at politiet er i kontakt med flere som ikke har norsk som morsmål enn de som har det? Dette aner jeg ikke, men la oss si at 9/10 som bor i Norge har norsk morsmål (...). Hvis antall som politiet er i kontakt med er likt fordelt så er det bare en tiendedel som er fra andre land eller som har utenlandsk bakgrunn. Da må modellene trenes med det for bilde. Men hvis det er sånn at halvparten som politiet har kontakt med er det, da må modellene trenes med det for øye.»

Bjørn viser til at en benektelse av virkeligheten potensielt vil kunne være farlig i seg selv og lage skjevheter i teknologier, som ikke vil gjenspeile det faktiske norske samfunnet. Dette mener han er et viktig aspekt i teknologiutvikling. Bjørn viser til at dette handler om graden av tillit samfunnet har til norske myndigheter. Hvordan forebyggende teknologibruk kan utfordre den eksisterende tilliten er en problemstilling flertallet av informantene beskriver i sine intervjuer. Dette vil derfor utdypes i den siste delen i kapittelet.

5.4.4 Tillit

I rapporten «I forkant av kriminaliteten» (Politidirektoratet, 2020, s. 18) skrives det at: «Politiet er avhengig av tillit for å kunne ivareta samfunnsoppdraget på en god måte. Innbyggernes tillit til politiet påvirkes av hvor effektivt og kompetent politiet er til å løse sine oppgaver, samt hvordan politiet opptrer i sin oppgaveløsning». Publikums tillit til politiet, til teknologi og til de som utøver kriminalitetsforebygging beskrives som spesielt viktig av flertallet av informantene. Som vist til tidligere i avhandlingen kan innsyn i forebyggende teknologi være krevende. Som også vist til tidligere kan dette handle om hvordan teknologien er bygd opp og hvilke vurderinger som er gjort i utviklingen av den, samt hvordan verktøyene faktisk fungerer i praksis. Manglende innsyn kan i sin tur resultere i manglende tillit i samfunnet ifølge Dina:

> «Jeg tror også at tillit kommer av transparens. Så hvis man får innblikk i beslutningene og hva man faktisk gjør. Mange tenker jo «worst case scenario» fordi man ikke vet, og når man ikke vet så tenker man at det er farligere enn det er fordi det er best å være føre-var kanskje. Jeg er jo ofte litt ekstra redd for ting jeg ikke kjenner til. Så jeg tenker at man må ha transparens i hele prosessen. Mellom aktørene så klart, men også ut til samfunnet da. Og at det er sånn som forskning er, at det skal ha de samme kravene til reproduksjon og at man kan ettergå resultatene. At man kan skjønne hva som ligger i at vi prøver å vise frem hva vi vet og hva vi ikke vet. Hva den blackboxen er og hva den ikke er. Og sånn tror jeg det er med alt, spesielt det som politiet gjør. Fordi hvis politiet gjør noe som folk ikke skjønner hvorfor de gjør, da får vi mistillit.»

Også Bjørn er inne på den samme tematikken:

> «Ja, enten det nå er at utlendinger ikke blir stoppet fordi vi nektet å skrive at utlendinger er mer involvert eller at de blir stoppet oftere. Begge deler er like ille. Fordi begge deler gjør seg veldig dårlig i mediene og dermed tærer det på en veldig viktig ressurs som er den tilliten politiet har.»

Cato beskriver på sin side dragningen mellom å få på plass nye forebyggende verktøy og det å skape en forsvarlig bruk av teknologi. Han mener at en forsvarlig bruk av teknologi er en viktig del av samfunnets tillit til politiet:

> «Også har du jo politidistriktene (...), som jo er eksperter på hvordan dette skal brukes i politisammenhenger og etterforskning og sånt. Så du har jo ulike miljøer som drar litt i ulike retninger hvor noen vil bruke ny teknologi som er veldig opptatt av å løse samfunnsoppdraget. Mens andre er opptatt av at det skal være innenfor jussen og at det skal være forsvarlig (...).»

Cato beskriver samtidig hvordan det tydelig er ulike interesser blant politiansatte. Slik Cato beskriver de ulike miljøene innad i politiet, vises det dermed også til ulike tilnærminger til tillitsbegrepet. Dette bekreftes av informanten Erik, som viser til at det finnes et stort spekter av hvordan en definerer tillit. Erik mener at dette gjør teknologiutvikling vanskelig.

Flertallet av informantene snakker altså om problemstillinger i forbindelse med tillit til teknologiene. De viser til at det er viktig å utvikle forebyggende teknologi forsvarlig, innenfor juridiske rammer og med åpenhet i bunn. Fredrik mener derimot at forebyggende teknologi ikke nødvendigvis er mindre tillitsfull enn generell forebyggende virksomhet. Dette gjør han ved å beskrive de høye kravene som stilles til forebyggende teknologiske verktøy. Fredrik mener at mennesker har en tendens til å sammenligne ny teknologi med det perfekte og ikke med «dagens situasjon». Dette begrunnes med følgende forklaring:

> «(...) har opplevd en del ganger vi har automatisert at folk blir veldig skeptisk når vi sier at den nye maskinen har 5 % feil, og da vil de ikke ha den. Men når vi undersøker dagens feilmargin når mennesker gjør jobben så er den 10 %».

Fredrik mener videre at mennesker eksempelvis uttrykker stor bekymring når et nyutviklet kunstig intelligent verktøy opptrer rasistisk i USA. Det interessante med dette, mener Fredrik er at «hvis man hadde undersøkt antall dommer der aktørene i rettsaken har vært rasistisk mot tiltalte av annen hudfarger og religion; så ville trolig ikke tallet lagt på null». Argumentasjonen til Fredrik avsluttes med å påpeke at «det er viktig å vurdere ny teknologi opp mot den virkelige verden, og ikke en ideell verden som ikke eksisterer». Fredrik sier altså at teknologien ikke vil være feilfri, men at dette heller ikke vil være tilfellet hos mennesker. Det skapes dermed et narrativ av at fraværet av skjevhet på generelt grunnlag vil være uoppnåelig. Fredrik knytter samtidig diskusjoner om rasisme opp mot tillitsbegrepet. Dette tydeliggjør hvor kompleks kriminalitetsforebygging er i utgangspunktet.

Med ny teknologi er ikke lengre kvantiteten av mengder informasjon en utfordring. Avhandlingen har vist at det finnes programmer og teknologi som kan prosessere svært store mengder data. Dilemmaet er dermed ikke hvordan vi skal samle inn nok informasjon, men om hvordan tillit og kontroll havner i konflikt med hverandre. Nye overvåkningssystemer bygger som vi har sett ofte på masseinnhenting av informasjon om mennesker. Tillit i moderne kriminalitetskontroll vil derfor ikke bare handle om holdningen til ny forebyggende teknologi, men også om det helhetlige rettssystemet. Prosessene rundt teknologiutvikling, implementeringen og bruken av den står sentralt. Gjennomgående i avhandlingen viser både informantene og forskningslitteratur til at tillit er helt avgjørende for at politiet skal kunne inneha posisjonen de har i det norske samfunnet i dag. Det betyr at forebyggende teknologiutvikling må drives frem på en måte som gjenspeiler dette. Et viktig spørsmål er hvordan dette skal la seg gjøre.

5.5 Hvordan tilrettelegge for tillitsfull teknologi?

I det siste analysekapittelet vil jeg undersøke hvordan det kan tilrettelegges for en tillitsfull bruk av teknologier innen kriminalitetsforebygging. Hovedpunktene er de momentene som informantene vektlegger i sine intervjuer. Dette er følgende: «datagrunnlag- små og store data», «kunnskap og kompetanse om teknologi», «samarbeid og tverrfaglighet» og «transparens».

5.5.1 Datagrunnlag – små og store data

Til tross for den raske spredningen av databaserte former for kunnskapsproduksjon, mener Flyverbom og Murray (2018, ss. 2-3) at vi så vidt har begynt å konseptualisere og forstå hvordan teknologien former verden rundt oss. Digitale spor blir i økende grad ansett som en primærressurs for verdiskapning, innflytelse og kunnskapsproduksjon. Likevel mener Flyverbom og Murray at vi i dag vet lite om prosesser rundt strukturering, sortering og kurering av data. De viser også til mangelen på forskning rundt konsekvensene av datastrukturering. Datastrukturering tolkes som digitale spor som er organisert på måter som gir mulighet for analyse, verdiutvinning og koblinger til ulik sosial produksjon eller politisk påvirkning. Det er i stor grad med på å forme menneskelig atferd og sosial orden. Flyverbom og Murray (2018, s. 3) mener at usynlige og tilsynelatende tekniske måter å håndtere data på, har store implikasjoner på hvordan mennesker, organisasjoner og instanser handler på grunnlag av data. De mener derfor at dette er viktig å rette oppmerksomheten mot.

Innledningsvis i avhandlingen er begrepet stordata introdusert og definert. Et sentralt spørsmål i dag er hvordan stordata vil omforme samfunnet, samt hvilke samfunnsmessige transformasjoner vi kan tilskrive stordata. En side av det er den økonomiske veksten det kan gi infrastruktur, produkter og tjenester. Dette betegnes gjerne som «dataøkonomi». Her sporer private selskap innbyggere med mål om å selge disse datasporene videre. Disse kan myndigheter kjøpe og ta i bruk for å drive overvåkning og kontroll (Zuboff, 2019). En annen side er fremveksten av nye sosiale og kulturelle formasjoner med utgangspunkt i data, deling og informasjon. Dette har blitt kalt fremveksten av «algoritmiske kulturer». Her får datamaskiner innpass i sorteringen, klassifiseringen og hierarkiseringen av mennesker, steder, objekter og ideer. I en slik omveltning ligger bekymringen for konsekvensene av det algoritmene produserer og mater ut i samfunnet (Flyverbom & Madsen, 2015, s. 142). Det har derfor blitt rettet oppmerksomhet mot de problematiske konsekvensene av å stole på stordata i sammenheng med regulering og politikkutforming. Morozov (sitert i Flyverbom og Madsen, 2015, s. 143) har uttalt følgende: «rise of data is the death of politics because it replaces politics, history and experience with a naive belief in data and algorithms». Morozov mener videre at hvis vi tar avgjørelser om helsetjenester, risikohåndtering og kriminalitetsforebygging ved å stole på digitale spor og algoritmiske beregninger, vil vi la «Silicon Valley-logikk» og teknokratiske visjoner undergrave viktige og langvarige prinsipper for samfunnsmessig og politisk styring. Dette inkluderer ifølge ham velferd, stat og demokrati.

Både manglende synlighet av bestemte data og skjeve data er dermed noe som kan vanskeliggjøre tillitsfull forebyggende teknologi. Dette er også noe informantene gjennomgående har trukket frem i sine intervjuer. Det har samtidig blitt beskrevet som farlig å lage uklare skillelinjer mellom idealer og forventninger til faktiske «harde data» og «soft intelligence data». Det å skulle støtte seg på data av dårlig kvalitet samtidig som man overser viktige rettigheter som retten til privatliv og personvern, er også ansett som problematisk (Fyfe, Gundhus, & Rønn, 2018, s. 13). Et viktig poeng er ifølge Fredrik at det må løftes opp krav til presisjon i data. Dette mener han er spesielt viktig når tiltak skal settes inn mot enkeltpersoner:

> «Når det gjelder forebyggingsdelen så mener jo jeg at altså.. (...) hvis du skal bruke informasjon til å fatte vedtak om enkeltpersoner, altså at det vil kunne ha en konsekvens for den enkelte, så er det i seg selv problematisk å benytte disse analyseformene som noe mer enn en input. Altså, de kan være en input på lik linje som andre kilder er en input, men det er et helt nytt spor som må går opp da tenker jeg. Et godt eksempel på

> det er dette her... da Justisdepartementet for ikke lenge siden hadde et lovforslag på høring som skulle gi PST adgang til å samle inn store informasjonsmengder fra åpne kilder for å kunne gjøre analyser på bakgrunn av det. Men i det lovforslaget, så vidt jeg husker, så var det både åpnet for at man kunne bruke det i forbindelse med saksbehandling knyttet til enkeltpersoner, og mer generelt og etterretning, som handler om å lage et mer overordnet informasjonsbilde. Og at det overordnede informasjonsbildet forteller noe om situasjonen der ute basert på åpne kilder, tenker jeg i utgangspunktet er uproblematisk for å si noe om for eksempel påvirkningsoperasjoner eller terrornettverk som kommuniserer på ulike lukkede forum og i åpne kilder. Men det er noe helt annet enn å bruke de samme dataene for å gjøre vurderinger og tiltak mot enkeltpersoner.»

Fredrik skiller altså mellom innsamling av åpne kilder og det som vil være mer inngripende innsamling av data som angår enkeltindivider. Utgangspunktet for det han beskriver, er proposisjonen (Prop. 31 L (2022-2023), ss. 5-6) fra Justis- og Beredskapsdepartementet. Den ble lagt frem for Stortinget i 2022 og ble senere godkjent i statsråd. Av proposisjonen fremkommer det et ønske fra Politiets Sikkerhetstjeneste (PST) om utvidede endringer i politiloven og politiregisterloven, samt at PST skal kunne lagre, systematisere og analysere store mengder åpent tilgjengelig informasjon på internett. PST skriver i proposisjonen at deres muligheter for forebygging i dag er begrenset. I proposisjonen skrives det samtidig at endringene «er avgjørende for at PST skal kunne analysere endringer i trusselbildet og vil bidra til at PST kan avdekke ukjente trusselaktører og oppdage nye fenomener som kan medføre nye trusler».

I proposisjonen (Prop. 31 L (2022-2023), s. 7) poengteres det samtidig at den sikkerhetspolitiske situasjonen i Europa er forandret etter Russlands invasjon av Ukraina. Her vises det til hvordan ekstraordinære hendelser åpner opp for et mer inngripende regelverk. Vi kan dermed trekke paralleller mellom dette og Kaufmans argumentasjon om hvordan diskurser om sikkerhet åpner opp for utvidede kriminalitetsforebyggende tiltak. Fredriks argumentasjon viser samtidig at kravene til datagrunnlag bør avhenge av formålet for forebyggingen.

Et flertall av informantene er opptatt av å trekke frem nettopp hvordan et godt datagrunnlag danner utgangspunkt for tillitsfull teknologi. Anne snakker om dette i sitt intervju:

> «For å gjøre alvor av å tenke og satse på forebygging basert på data som politiet besitter, så tror jeg at de dataene må behandles på en annen måte med det også som formål for å sørge for at man har et datagrunnlag som er godt nok.»

Anne beskriver at prosessen rundt det å skulle samle inn datamateriale kan være krevende. Hun mener at man risikerer å kun sitte igjen med en liten mengde data dersom det kun skal benyttes data som er relevant for teknologien. Anne sier også at dersom teknologiens hensikt er maskinlæring, vil ikke nødvendigvis all dataen være egnet som maskinlæringsmateriale. Skal man satse og skaffe seg erfaring med kriminalitetsforebygging på grunnlag av data fra norsk politis egne systemer, mener hun at det er viktig å se på hvordan man arbeider rundt teknologi, struktur og databehandling. Anne beskriver også konsekvensen av å ikke ha godt datagrunnlag:

> «Men en veldig viktig del av det er nettopp det at et dårlig datagrunnlag øker risikoen for at politiet feiler i andre retninger når man ikke er i stand til å detektere det man tror man skal detektere, eller at man ender opp med falske positiver og plager folk som ikke skulle vært plaget.»

Anne bruker her begrepet «dårlig datagrunnlag». Flere av de øvrige informantene snakker også om kvaliteten på datagrunnlag innen forebyggende teknologi. Det er derfor interessant å undersøke hva informantene legger i dette. Dette er noe Dina går nærmere inn på i sitt intervju. I diskusjonen rundt datagrunnlag tar hun utgangspunkt i geografisk analyse. Dina viser til at man i teknologiutvikling må undersøke om andre faktorer enn de som er integrert i datamodeller også kan være relevante. Dina nevner anmeldelsestilbøyelighet som eksempel på en viktig faktor som ikke nødvendigvis synes i dataene til geografiske analyser. På tross av dette kan nettopp anmeldelsestilbøyelighet ha mye å si for hvor mye kriminalitet som måles i et bestemt område. For å ha et best mulig datagrunnlag beskriver hun at det er mulig å innhente data fra ulike registre som ikke er direkte koblet opp mot politiets egne systemer. Dette er i tråd med Kaufman, Egbert og Leese (2018, s. 681), som viser til at det er ulike korrelerende mønstre som brukes til å forutse kriminalitet. Dina mener at slike korrelerende mønster kan styrke en datamodell som skal forutse forekomsten av lovbrudd på bestemte lokasjoner.

Dina forklarer at en del av teknologiutviklingen hun driver med, er å se på de ulike muligheter og begrensninger data kan gi. Dette er noe flere av informantene snakker om i sine intervjuer.

En av teknologiene som diskuteres i et flertall av intervjuene er Nettprat-prosjektet. Dette ble gjennomført i et samarbeid mellom Politihøgskolen og Trøndelag politidistrikt. Formålet var å undersøke om data i straffesaker om seksuelle overgrep som omhandlet barn, var egnet som treningsdata for å utvikle et forebyggende verktøy. Verktøyet skulle baseres på maskinlæring. Helt konkret undersøkte prosjektet om chattelogger sikret som bevis i slike straffesaker, kunne brukes for å utvikle teknologi for forebygging av nettovergrep mot barn. Dette skulle gjøres ved å benytte nettprat-bevis innhentet i etterforskning som treningsdata til en lærende KI-modell (Sunde, Bendiksen, & Sunde, 2022, s. 8).

Chatboten ble i prosjektet kalt en PrevBOT. Dette var en intelligent chatbot som kunne settes ut i offentlige chatrom på internett. Boten hadde til hensikt å analysere åpent tilgjengelig informasjon i form av opplysninger i brukerprofiler og i chat-samtaler. På bakgrunn av dette kunne chatboten for det første varsle om forekomsten av samtaler mellom voksne og barn. For det andre kunne boten fange opp hvorvidt deltakere som opptrådde som barn mest sannsynlig var voksne, og/eller med et annet kjønn enn oppgitt. Til slutt kunne det varsles dersom tidligere domfelte gjenopptok ulovlig adferd på internett. PrevBOTens formål ble begrunnet med å kunne være et nyttig verktøy for å avdekke problematiske nettsted eller fora, samt fange opp individer som kunne være spesielt risikable for barn. På denne måten kunne politiet drive forebygging over internett. Et sekundærformål var at chatlogger og annen lagret data kunne gi grunnlag for etterforskning. Dette kunne særlig gjelde hvis mistanken omhandlet en serieovergriper (Sunde, Bendiksen, & Sunde, 2022, ss. 11-12).

Det er interessant å se hvilke utfordringer som ble avdekket i Nettprat-prosjektet. Vi kan blant annet se at et lite egnet datagrunnlag var en av hovedproblemstillingene som ble funnet. Ulik praksis mellom ulike politidistrikt i håndteringen av data sikret som bevis var også noe som ble trukket frem i etterkant av prosjektet. Nettprat-rapporten viste til at datatilfanget varierte i fullstendighet og kvalitet. Som konsekvens av dette fikk man svekket kvalitet i bruken av treningsdata for en lærende algoritme. For å utvikle forebyggende verktøy basert på maskinlæring viser Nettprat-rapporten til at det stilles kvalitetskrav til datagrunnlaget: «det må være relevant, representativt, feilfritt, komplett og ha egenskaper som gjør det egnet for statistiske analyser» (Sunde, Bendiksen, & Sunde, 2022, s. 41).

Nettprat-prosjektet resulterte i relevante data, men en mindre mengde data enn forventet. Årsaken var at det både var tidkrevende og komplisert å identifisere saker med relevante data

for prosjektet. På generelt grunnlag krever uthenting og bearbeiding av data mye manuelt arbeid. Det var også store skjevheter i datagrunnlaget som ble hentet ut; der lå blant annet et fåtall saker som skilte seg ut, med mye data som involverte en gjerningsperson og mange fornærmede. Hadde et slikt datagrunnlag vært benyttet i praksis, ville dette kunne resultert i skjeve data. I tillegg viste kvaliteten på nettpraten i straffesakene seg å være svært varierende og mye var av lav kvalitet. En stor andel av nettsamtalene stammet fra tjenesten «Snapchat», noe som hadde betydning for fullstendigheten og omfanget i nettsamtalene. «Snapchat» er en tjeneste uten logging, og som i hovedsak består av skjermbilder eller lagrede enkeltmeldinger. På grunn av de nevnte utfordringene i prosjektet, ble det ikke anledning til å igangsette utvikling og testing av en maskinlæringsmodell på grunnlag av de innhentede dataene. Det var heller ikke mulig å konkludere hvorvidt datagrunnlaget var tilstrekkelig eller av god nok kvalitet (Sunde, Bendiksen, & Sunde, 2022). I rapporten vises det til følgende:

> Datainnhenting i etterforsking ivaretar ikke behovene som reiser seg for å kunne utøve kunnskapsbasert forebygging av nettbaserte overgrep basert på kunstig intelligens. Vi understreker derfor at for å kunne ha et egnet datagrunnlag til å utvikle forebyggende KI-baserte politiverktøy, må politiet tenke nytt om behandlingen av slike data (Sunde, Bendiksen, & Sunde, 2022, s. 54).

Cato understreker i sitt intervju betydningen av at datagrunnlag må være av god kvalitet for at input-data skal komme ut på andre enden som tillitsfulle output-data. I forbindelse med Nettprat-prosjektet hevder Cato at mangelen på tilstrekkelig datagrunnlag kan resultere i at individer som ikke skulle vært plukket opp, likevel blir det. Dette er i tråd med Annes argumentasjon rundt Nettprat-prosjektet; nettopp at man risikerer falske positiver:

> «Men det er klart at hvis du kommer med pekefingeren på mange som kun holder på med uskyldig prat så vil ikke folk være der. Da tar du jo bort en mulighet som mange setter pris på da. Så det å finne den balansen i systemet og kunne lære det.»

Andre fremhever at det er positivt at prosjektet synliggjorde at den lærende algoritmen trolig ikke ville vært treffsikker nok. Dina påpeker at hvis man treffer feil med dataene i utgangspunktet, så vil det trolig fortløpende dukke opp ulike etiske utfordringer. Dinas tolkning er at slike etiske utfordringer vil være misvisende når det kommer til opprettholdelsen av tillit i samfunnet. Hun sier samtidig at hvis det ender opp med at flere føler seg overvåket enn det

som kanskje er tilfellet, vil teknologien treffe feil. Dinas utgangspunkt er at et egnet datagrunnlag generelt sett er noe som kan bygges opp over tid. Videre viser hun til at dette er noe som kan åpne opp for flere teknologier som kan implementeres på et senere tidspunkt. Dina mener derfor at det er positivt å utvikle og teste ut nye forebyggende verktøy. På denne måten kan teknologien utbedres og kvalitetssikres før den tas i bruk i samfunnet. Dina viser samtidig til at en slik uttesting danner et kunnskapsgrunnlag som kan vise seg nyttig for norsk politi, og eksemplifiserer hvordan Nettprat-prosjektet kan ha en forebyggende effekt i fremtiden.

Fredrik forteller i sitt intervju hvordan kunnskap om teknologi kan styrke et datagrunnlag. Dette kan ifølge ham gjøres gjennom å teste ut ulike teknologier i såkalte «sandkassemiljøer». Han viser til hvordan det er mulig å bygge opp ulike datamodeller, for så å putte treningsdata inn i disse. På denne måten kan man drive uttesting av teknologi, uten at teknologien faktisk er implementert i praksis. I et slikt sandkassemiljø vil man kunne kontrollere omgivelsene og oppdage potensielle feil i treningsdataene man har puttet inn. Fredriks beskrivelser favner en del av det Datatilsynet driver med i dag; Datatilsynet viser til at det de omtaler som «regulatoriske sandkassemiljøer», kan bidra til å øke kunnskapen og fremme utviklingen av gode løsninger for kunstig intelligens. Et slikt «testmiljø» vil dermed kunne bidra til utviklingen av teknologi, samtidig som personvernet ivaretas. På denne måten vil man kunne drive frem teknologiutvikling på en tillitsfull måte. Datatilsynet viser til at dette er noe som kan gi innsikt i nye innovative løsninger, samt gjøre det lettere å identifisere potensielle risikoer på et tidlig stadium av teknologiutviklingen (Datatilsynet, 2020). Både Fredrik og Dina viser altså til en sammenheng mellom datagrunnlag og kunnskap om teknologi. Kunnskap om forebyggende teknologiutvikling vil derfor diskuteres i neste delkapittel.

5.5.2 Kunnskap og kompetanse om teknologi

Gjennomgående i intervjuene dukker viktigheten av kunnskap og kompetanse om teknologiutvikling opp. Dette beskrives som avgjørende for at politiet skal kunne benytte forebyggende teknologier for å forhindre kriminalitet. Forskning viser til at i teknologiutvikling, vil kunnskap om teknologiens virkemåte, potensielle feil og slagsider, samt ferdigheter i interaksjon med systemene være nødvendig (Klepper, et al., 2021, s. 30). Det fremheves at dette må skje på en måte som «ivaretar tillit og legitimitet i befolkningen» (Klepper, et al., 2021, s. 13). Vi kan dermed se hvor viktig tillitsbegrepet er i denne sammenhengen. Behov for kunnskap og kompetanse er også i tråd med Vestby og Vestbys (2019, ss. 7-8) ståsted:

> As a society we have an interest in crime prevention and efficient policing, but we also have an interest in ensuring that law enforcement strategies, including deployment and surveillance decisions, are effective, fair, and just. This requires understanding, testing, and governance.

Cato vektlegger at mye av skjevheten og kritikken mot teknologi, handler om manglende kunnskap om hva teknologien faktisk er. Innledningsvis i analysen ble informantenes definisjonsavklaring av kunstig intelligens presentert. Cato forklarer at kunstig intelligens egentlig bare er et dataprogram som er nyttig hvis man får det til å fungere innenfor de etiske rammene man ønsker å ha, og innenfor målplanene en setter opp. I likhet med Cato, mener også Dina at kunstig intelligens er noe som høres mer innviklet ut enn det egentlig er:

> «Jeg selv tenker at KI er noe som høres komplisert ut, også er det egentlig veldig enkelt. Så sånn er det med mye forskning som forsøker å ha sine begrepsavklaringer.»

Cato mener på sin side det er viktig å teste ut teknologi før man eventuelt «ruller» teknologien ut på norske borgere. Nettprat-prosjektet og regulatoriske sandkassemiljøer som tidligere er diskutert, er eksempler på en slik uttesting; her blir potensielle skjevheter synliggjort, og styrker og svakheter ved teknologien blir avdekket. Kunnskap om hvordan teknologi er bygd opp og fungerer, vil på denne måten være et svært viktig ledd i tillitsfull forebygging.

Gjennom avhandlingen har det blitt vist til hvordan den teknologiske omveltningen har påvirket kriminalitetskontrollen. Det er ikke bare forebygging av lovbrudd som gradvis har forflyttet seg over til teknologiske løsninger, men også noen typer lovbrudd:

> Den organiserte, skjulte kriminaliteten synes å utvikle seg i takt med den teknologiske utviklingen i samfunnet, og synes å bli stadig mer kompleks, vanskeligere å oppdage og mer utfordrende å etterforske. Vi registrerer også at den kriminalitet som begås på internett ved hjelp av kryptert kommunikasjon og kryptert valuta utfordrer politiets metoder innen kompetanse, kapasitet og teknologi (Klepper, et al., 2021, s. 9).

Erik snakker om nettopp dette i sitt intervju og eksemplifiserer det med en tidligere sak som har preget nyhetsbildet: I 2018 ble Anne-Elisabeth Hagen bortført fra hjemmet sitt i Lørenskog. I etterkant av kidnappingen ble det fremmet et anonymt løsepengekrav. Dette ble gjort via

kommunikasjon i kryptovalutaen «monero» (Brekke & Helljesen, 2020). Løsepengekrav gjennom kryptovaluta er et stadig mer utbredt fenomen. Dette fordi slike valutaer er anonyme og uregulerte, samt at politimyndigheter har vanskeligheter med å følge transaksjoner eller fryse digitale midler (Johannessen, 2019). Erik forklarer at det har krevd store ressurser for politiet i Lørenskog-saken å skaffe kompetanse om kryptovaluta. Han sier at til tross for at det kanskje ikke vil være mulig for politiet å løse den aktuelle saken, vil etterforskningen som ble gjort kunne gjøre det enklere å løse lignende saker i fremtiden. Erik forklarer at etterforskningen foregikk i Øst politidistrikt, og at det derfor vil være en fordel å drive kunnskapsdeling på tvers av ulike distrikter. På denne måten skapes det kunnskapsflyt innad i politiet. Dette mener han kan være spesielt viktig for teknologisk kompetanse, som han betegner som et krevende fagfelt. Erik viser til hvordan kompetanse om teknologi kan ha en fremtidig forebyggende effekt på kriminalitet.

Cato sier i sitt intervju at det er svært viktig å undersøke hvilke områder forebyggende teknologi faktisk skal anvendes og hvordan den skal anvendes. Cato beskriver også hvordan de algoritmene som gjerne finnes i slike teknologiske verktøy, er svært komplekse. Dette har ifølge ham sammenheng med kunnskapsgrunnlaget, og hva som er output og input av systemet. Cato mener at dette vanskeliggjør opparbeidelse av kunnskap om teknologi:

> «La oss si i det tilfellet her da; programvare levert av Palantir hvor man kanskje ikke har god nok kontroll på algoritmene og hvordan dataene behandles. Det er noe helt annet enn å utvikle ting selv, hvor du kan redegjøre i detalj hvor ting er utført og satt opp. Derfor bygger (...) jo blant annet opp et stort IT-miljø i politiet i dag, (...) for å være i stand til å ha bedre kontroll selv da. Men veldig mange IT-systemer fungerer jo som en black box. Og KI-algoritmer er jo for de aller aller fleste en black box, og spørsmålet er jo kanskje om alle er det. Altså, fordi algoritmene som ligger der er så kompliserte at de færreste, om noen har et godt innsyn i hvordan de faktisk fungerer og hvordan outputen produseres da. Så det i seg selv er jo et interessant tema å se på; «finnes det forklarbare modeller som gjør at resultatet kan forklares tilbake til input-dataene?» eller sitter vi alltid med en sånn black box der? (...) det er kjempespennende tema.. og komplisert og stort.»

Når Cato bruker begrepet «black box», viser han til input- og output-data som er ukjent for andre enn de som legger inn dataen i et system. Mer nøyaktig kan dette beskrives som ukjente

variabler som en programvare behandler. Det er disse variablene som vil avgjøre hvorfor en maskin gir den informasjonen den gir eller utfører de handlingene den gjør (Leese, 2014, s. 504).

Flyverbom og Madsen (2015, 146) trekker en linje mellom data og kunnskap. De peker på fire sentrale elementer i forbindelse med dette; det første omhandler produksjon av data. Dette er trinnet hvor menneskelig oppførsel og bevegelse av objekter blir oversatt til en kvantitativ og binær strøm som kan lagres og behandles av en datamaskin. Det andre momentet er struktureringen av data. Dette involverer valg av databaser, klassifiseringssystem og metadata som data kjøres gjennom og klargjøres for systematisk analyse. Det tredje trinnet gjelder distribusjon av data. Mer spesifikt er dette måten tilgang til databaser og distribusjon av digitale spor føres mellom dataeiere og sluttbrukere. Sistnevnte moment er visualisering av data. Dette innebærer valg om hvordan man kan gjøre tilgjengelige data om til visualiseringer, som kan gi innsikt i de aspekter man er interessert i. Alle disse prosessene vil være viktig å ha kunnskap om. Synliggjøring av teknologiske prosesser fremheves som en viktig del av tillitsfull teknologiutvikling.

Innenfor maskinlæring og kunstig intelligens har såkalte «black boxes» blitt omtalt som problematiske. Utgangspunktet er at de vil medføre et tap av sporbarhet for borgere i samfunnet (Leese, 2014, s. 504). Dette kan for det første resultere i at det stadig blir vanskeligere å etterprøve teknologien. For det andre vil det kunne medføre diskriminerende praksis uten at dette blir oppdaget. Til slutt vil det også være krevende å skulle sørge for borgeres personvern (Leese, 2014, s. 496). Samtlige nevnte problemstillinger er diskutert i denne avhandlingen. Dina mener på tross av omtalt problematikk rundt «black boxes», at slike ukjente algoritmer ikke nødvendigvis er så kompliserte som en gjerne skal ha det til:

> «Men jeg har fått snakket med mange som arbeidet med dette og lært hvordan utregningene fungerer. Også høres det jo veldig vanskelig ut, men så finner man ut at det egentlig ikke alltid er det. Så mye av det som blir fremstilt i debatten som sånn «black box» eller «dette aner vi ikke», så sitter jeg og hører på sånne foredrag av og til, og da tenker jeg «jo at dette kan jeg jo forklare, eller det vet jeg at jeg kan se i dataene hvordan fungerer». Så hvis man ikke har et samarbeid mellom folk med ulik kompetanse, så blir det selvfølgelig masse store «black box». Fordi jeg har jo en «black box» på ting du vet, og du har en på det jeg vet. Men hvis vi jobber sammen så tenker jeg at boksene som man tror er der kan bli mye mindre da. Og det har jo vært litt sånn

> fellesnevneren med disse metodene; at «vi vet ikke hvordan de fungerer», også er det kanskje fordi det er vanskelig å skjønne hvis man ikke har satt seg inn i dataene eller metodene selv da. Så da gjelder det å ha et samarbeid med noen som kan det litt bedre.»

Utgangspunktet til Dina er at det er oppnåelig å skaffe seg kunnskap og kompetanse rundt forebyggende teknologi, til tross for at teknologien kan fremstå kompleks. Politiet beskriver selv et behov for et godt kunnskapsgrunnlag som kan bidra til å redusere usikkerheten rundt prioriteringer og beslutninger om tilnærming og valg av forebyggende tiltak (Politidirektoratet, 2020, s. 22). Et sentralt spørsmål er dermed hvordan man kan sikre muligheten for nødvendig kompetanse og kunnskap. Dina mener at dette er mulig ved hjelp av en tverrfaglighet hos de som arbeider med denne typen teknologi. Dinas tolkning er i tråd med forskning på området: « (…) to promote an effective and legitimate security governance, requires the regular involvement of a broader set of disciplines with their sensibilities and theoretical insights in the evaluation of technologically mediated policing.» (Niculescu-Dincă, 2021, s. 97). Dette vil jeg nå se nærmere på.

5.5.3 Ansvarsfordeling og tverrfaglighet

FFI-rapporten fra 2021 (Klepper, et al., s. 3) viser til at det er lite tverrfaglig kompetanse på teknologiutvikling hos politiet. Det etterlyses samtidig flere ansatte med teknisk kompetanse. Rapporten avdekker også at det på tross av dette, finnes et tydelig ønske om å bruke teknologi og utvikle løsninger for å forbedre politi- og påtaletjenestene. I tillegg vises det til at mange innad i politiet i større grad ønsker en tverrsektoriell samhandling med øvrige arenaer for en slik interaksjon.

Flere av informantene er inne på dette. Bjørn etterlyser en klar ansvarsfordeling innen teknologisk utvikling, og spesielt innen utvikling av kunstig intelligens og maskinlæring. Bjørn stiller også spørsmålstegn ved hvilke aktører som egentlig bør være involvert og sørge for en riktig bruk av KI i politiet. Han påpeker at dette ikke står spesifisert i noen form for politistrategi. Bjørn er her inne på et viktig poeng; for at politiet skal gjennomføre sitt samfunnsoppdrag i form av forebygging, er det helt nødvendig med en klar ansvarsfordeling. Bjørn mener at det er her kjernen ligger for å skape tillitsfull teknologi. Behovet for tverrfaglighet innad i politiet beskriver også av øvrige informanter:

> Dina: «Ja, og altså jeg har holdt på med det i mange år og jeg også lærer fortsatt. Og jeg også får jo masse ut av å snakke tverrfaglig. Det er altså kjempebra. Tverretatlig er enda bedre, fordi da får man begge deler.»

Vestby (2018, s. 266) mener at faglitteraturen om kunnskapsarbeid i politiorganisasjoner har avdekket utfordringer i informasjonsflyten mellom ulike aktører, og trekker frem at analytikere ikke har fått innsyn i sensitive opplysninger, samtidig som politiet får for lite analytisk kunnskap. Dette støttes opp av FFI-rapportens funn som er beskrevet innledningsvis i dette delkapittelet. Det er også i tråd med det Dina beskriver:

> «For man prater jo fra ulike ståsted. Så da er det er vanskelig. Og det er jo vanlige interaksjoner i hverdagslivet også, hvis man har helt ulike utgangspunktet fra når man begynner å diskutere noe. Da skjønner man jo ikke hva den andre mener med sine argumenter. Så det som er viktig å få plass i starten av et sånt samarbeid og i forsking generelt er jo som jeg prøver å gjøre da; det å fortelle politiet eller andre forskere hva det er vi kan gjøre med akkurat de metodene jeg prøver. Hvilke begrensninger er det og hvordan kan vi gjøre sånn at disse presterer bedre, og kanskje bedre enn en person som kanskje har bias og andre ting som er problematisk.»

I en slik diskusjon blir også deling av informasjon mellom ulike etater og distrikter spesielt viktig. Som Cato beskrev i Lørenskog-saken, vil kunnskapsutveksling i politiet kunne fremme politiets tverrfaglighet. Etablering av dette innad i polititjenestene og utad mot andre sektorer, både innenlands og utenlands, vil kunne fremme den teknologiske omstillingen som foregår i dag (Klepper, et al., 2021, s. 3).

Vi kan også finne øvrige eksempler på hvordan samarbeid preger forebygging i den digitale sfæren: I 2018 avdekket politiet at det hadde blitt lastet ned eller delt overgrepsmateriale av barn fra 115 ulike IP-adresser i Agder fylke. Operasjon «Dark room», som den ble kalt var dette året den høyest prioriterte oppgaven for Agder-politiet. Arbeidet ble gjort tverretatlig av etterforskningsledere, analytikere, etterforskere med kompetanse og erfaring fra seksuelle overgrep og etterforskere fra ulike driftsenheter i politidistrikter. Også Kripos gikk etter hvert inn og bisto. Mange av sakene som ble avslørt omhandlet personer i Norge som bestilte overgrep over internett. Politiet avdekket også chattelogger der personer diskuterte å reise til utlandet for å begå fysiske overgrep mot barn. Politiet uttalte i ettertid at de håpte at dette ville

virke forebyggende: «Vi vet fra forskning at overgripere gjerne utvikler seg fra å være en nedlaster til å bli en overgriper. Hvis vi kan stoppe dem på et tidlig tidspunkt håper vi at det kan ha en forebyggende effekt» (Ditlefsen, Arntzen, & Egeland, 2018). Vi ser hvordan norsk politi mener at økt oppdagelsesrisiko vil kunne ha en forebyggende effekt.

Politiet har i etterkant av saken ytret ønsket om bedre internasjonalt samarbeid. Politiet viser til at «Dark room» har store internasjonale forgreininger. Det gjør at politiet må samarbeide med andre vestlige land, og med landet hvor overgrepet finner sted. Politiet mener at slike saker synliggjør behovet for «gode systemer for samarbeid». Norske myndigheter viser også til behovet for nasjonale føringer for hvordan slike saker kan løses best mulig i fremtiden (Otterlei & Øystese, 2017). Vi ser dermed viktigheten av både tverretatlig og internasjonalt samarbeid i forebyggende politiarbeid. Et systematisk og godt regelverk har samtidig vært etterlyst (Otterlei & Øystese, 2017). Dette kan handle om at denne typen lovbrudd er et relativt nytt fenomen som har hatt sitt inntog sammen med tilgjengelig teknologi. Forebygging av slike lovbrudd skiller seg dermed fra tradisjonelt politiarbeid som har mer etablerte føringer.

Gro beskriver i sitt intervju teknologiutvikling som en intrikat prosess:

> «Ja, og på en del av de nyskapningene vi holder på med så venter vi også litt på juristene og at de skal gi klarsignal da. Så vi er jo veldig tunge juridisk sett i politiet. Det er en veldig sånn rettslig prosess hvor vi vil gjøre alt mer enn riktig. For vi lever jo av tillit, så vi tar ingen sjanser. Det betyr jo også at ting går saktere, fordi vi ikke har nødvendig kompetanse i politi-Norge på jus, og man har jo heller ikke det i Europa. Så det her er ikke bare i Norge vi sliter med dette. Men jeg synes det er veldig artig å se fremgang og bevegelse. Det er helt fantastisk.»

Gro peker på viktigheten av juridisk kompetanse for å få til en tillitsfull bruk av forebyggende teknologi. Dette er noe som også trekkes frem i FFI-rapporten (Klepper, et al., 2021, s. 43): Her skrives det at både lovgivning og retningslinjer kan hemme den digitale transformasjonen innad i politiet. Det vises til den store avstanden som kan finnes mellom teknologiens muligheter og de juridiske begrensninger. Det foreslås at jurister involveres i den teknologiske utviklingen på et tidlig stadium. På denne måten kan teknologiforståelsen øke på juridisk side, samt at det kan legges til rette for maksimal realisering av teknologiske muligheter innenfor de juridiske rammene som finnes.

Gro trekker veksler på to viktige elementer. For det første beskriver hun viktigheten av kompetanse om teknologi. Dette faller innunder tematikken som tidligere er diskutert i avhandlingen. For det andre fremhever hun at tverrfaglighet i politiet er nødvendig for å kunne skape tillitsfull forebyggende teknologi. Cato er også inne på den samme tematikken:

> «Ja, og det er akkurat det jeg ser, som kanskje er noe at det største problemet med det vi snakker om da; at det krever enorm ekspertkompetanse sånn at folk utenfor nesten ikke er i stand til å gjøre seg opp en mening med mindre du setter deg ned og leser store og omfattende rapporter om det. Fordi alle disse små nyansene som vi snakker om nå, det har ikke folk flest et forhold til. Og da blir det jo også veldig vanskelig å ha en god diskusjon om det. Men et sted å begynne er jo å være mer transparent om det. Å bidra til å opplyse folk også sant.»

Cato viser til kompleksiteten i teknologi, samt utfordringene ved å tilegne seg nødvendig kunnskap. Cato mener at et viktig sted å starte er ved en transparens til teknologiutvikling. Hvorfor transparens spiller en viktig rolle i tillitsfull bruk av forebyggende teknologi vil være sistnevnte element som jeg diskuterer i analysen.

5.5.4 Transparens

Kaufman, Egbert og Leese (2018, s. 687) viser til at mønstre i algoritmer vil uttrykke og gjenspeile ulike antakelser om kriminalitet. Disse mønstrene vil ha lett for å bli maskerte og dermed skjule underliggende begrunnelser og skjevheter. Konsekvensen av dette er at det er lett å overse «den rene visuelle overflaten» som skjuler mønstrene. Dette er i tråd med det avhandlingen hittil har avdekket. På den andre siden vises det til at teknologi i sin tur faktisk kan avsløre eksisterende problemer med skjevheter i tradisjonelt politiarbeid. Dette vil favne en sentral del av det informantene snakker om i forbindelse med transparens i dette delkapittelet. Generelt vil også teknologi kunne føre til større eksponering og åpenhet om slike feil. I mange tilfeller har teknologi potensialet til enten å forverre organisatoriske feil eller rette på dem. Dette betyr at riktig bruk av teknologi er en nødvendighet for politiet om de ønsker å opprettholde tilliten i samfunnet (Klepper, et al., 2021, s. 109).

Et begrep som har vokst frem som følge av teknologiens potensielle negative implikasjoner er «data justice». Dette innebefatter et rammeverk for å forstå hva som står på spill i den økende

avhengigheten til datadrevne teknologier. Det forutsetter en god forståelse av hvordan ulike sorteringsmekanismer fungerer, samt deres korrelasjon til historiske kontekster, sosiale strukturer og dominerende agendaer. Utgangspunktet i en slik datarettferdighet er å ta hensyn til strukturell ulikhet og fremheve ujevnheter som forekommer på tvers av grupper og samfunn (Dencik & Sanchez-Monedero, 2022, s. 2). Premisset er at utviklingen innen data ikke kan betraktes separat fra sosial rettferdighet, men må integreres som en del av dette (Dencik & Sanchez-Monedero, 2022, s. 3). Et slikt fokus på datarettferdighet har i dag spredd seg til å bli interdisiplinært. Det vises også til at datarettferdighet har vist seg spesielt gjeldende i konteksten av stordata, kunstig intelligens og maskinlæring (Dencik & Sanchez-Monedero, 2022, s. 2).

Ingen av informantene nevner konkret begrepet datarettferdighet i sine intervjuer. Likevel kan mye av det som inngår i «data justice» knyttes til informantenes tolkninger av tillitsfull teknologi. Åpenhet rundt teknologiers skjevheter, bias og innebygde samfunnsstrukturer som kommer til uttrykk i teknologien, er viktig i informantenes beskrivelser. Et annet viktig moment som ofte nevnes av informantene, er transparens. Dette regnes som et viktig dataetisk aspekt innen datarettferdighet. Dina sier følgende:

> «Jeg tror at tillit kommer av transparens. Så hvis man får innblikk i beslutningene og hva man faktisk gjør (...) man tenker jo worst case scenario fordi man ikke vet, og når man ikke vet så tenker man jo at det er farligere enn det er fordi det er best å være føre-var kanskje. Jeg er jo ofte litt ekstra redd for ting jeg ikke kjenner til. Så jeg tenker at man må ha transparens i hele prosessen».

Også Cato mener at dette er helt avgjørende for en trygg teknologibruk:

> «Men det jeg tror er avgjørende er å være åpen om hva det er man bruker det til og på hvilke områder. Og hvordan det brukes. Altså, rett og slett at man redegjør for det da. Altså, jeg tenker jo at det er helt uproblematisk å si at at du bruker disse teknologiene hvis du redegjør i detalj for nettopp de tingene jeg sa. Og det i seg selv er jo tillitsvekkende. Problemet er jo at hvis du har en antagelse om at det brukes, men du aner ikke til hva.. du vet ikke hvordan det brukes eller hva det brukes til (...).»

Videre gir Cato et konkret eksempel og snakker om Entry/Exit-System som er beskrevet tidligere i avhandlingen. Cato forklarer at EU er åpne om de nye systemene sine for

grensekontroll inn og ut av Schengen. Hans tolkning er at dette handler om at EU selv er klar over at det er teknologi som er implementert på en god måte og at dette gjør det uproblematisk for EU å dele informasjon om teknologien. Cato mener at utfordringer med transparens først oppstår hvis det er usikkerhet rundt de juridiske og etiske sidene ved teknologien. Da mener han at det vil være større risiko ved å dele slik informasjon. Cato forklarer at hvis det er en åpenhet om de utfordringene som finnes i bestemte teknologier, vil vi samtidig kunne få en debatt rundt dette. Cato mener at dette i seg selv vil kunne bidra til å korrigere utviklingen av manglende gjennomsiktighet i samfunnet.

Dette er i tråd med Bjørns beskrivelser. Bjørn viser til at det finnes etablerte skjevheter i samfunnet i dag. I likhet med Cato mener han at det er en forutsetning for tillitsfull teknologi at vi har en åpen diskusjon om teknologi:

> «Vi må være helt åpne med at det er sosiale, rasemessige og mange andre aspekter som må på bordet. Vi kan ikke late som at, vi kan ikke si at «nei, vi er så nøytrale at vi tar ingen sånne hensyn. (...). Og når vi ser på hvem politiet er i kontakt med så er det sånn og sånn. Derfor velger vi ut de og de, når vi trener en modell. (...) det viktigste er at det er klart, og så er det nøye diskutert. Det er ikke bare sånt man finner ut etterpå. Det er en del av dokumentasjonen; hvem har bestemt det og hvorfor, med hvilken begrunnelse. Og så videre. Så jeg tror at det er mulig. Jeg tror det er mange ting som du kan handle i butikken og som du kan gjøre på telefonen som blir vanskelig å gjøre på en trygg måte eller på en god måte. Og når jeg sier trygg, så mener jeg ikke at det ikke virker. Men da mener jeg at det tåler, på en måte, medienes søkelys da. Det mest mistenkelige lyset det kan settes på, og at det tåler det. Og at det ikke er noen «vi vet ikke»».

Bjørn viser til samfunnstilliten som må opprettholdes og sier at politiet må sørge for at ingenting slipper videre før de har tenkt på alt rundt en mulig teknologisk løsning. Bjørn mener at dette også må gjelde for de mer kritiske aspekter i samfunnet, som diskrimineringsproblematikk. Vi kan se tydelige paralleller mellom Bjørns tolkning av tillitsfull teknologi og datarettferdighet:

> To speak of data justice is thus to recognize not only how data, its collection and use, increasingly impacts on society, but also that datafication is enabled by particular forms of political and economic organization that advance a normative

> vision of how social issues should be understood and resolved. That is, data is both a matter *in* and *of* justice; datafication embodies not only processes and outcomes of (in)justice, but also its own justifications (Dencik & Sanchez-Monedero, 2022, s. 3).

Tidligere i avhandlingen har teknologiers utfordring med hensyn til tillit blitt diskutert. Dette er også noe som informantene er opptatt av i sine intervjuer. Anne mener i likhet med øvrige informanter at det er viktig å ha fokus på diskusjonene rundt teknologibruk. Dette er i tråd med Vestby og Vestbys (2019, s. 1) ståsted, som er vist til i kapittel 2; de viser til viktigheten av å stille kritiske spørsmål til politiets bruk av prediktive analyser og programvarer. Anne påpeker at slike diskusjoner ikke bare er sentrale når forebyggende løsninger rulles ut, men også i utviklingen av dem. Spørsmål som «hvor mye ressurser vi skal bruke på teknologiutvikling?», «hvor nøye skal vi være?» og «hvor transparente skal vi være i utviklingsprosessen?» er viktig å stille. Anne mener at dette er etiske aspekter som er tett knyttet til politiet samfunnsoppdrag om å forebygge kriminalitet. Informantene viser til at det må være en gjennomsiktighet i hvordan data utvikles og brukes, til dataenes formål og til de sannsynlige implikasjonene av teknologibruk. Transparens er derfor tett knyttet opp mot tillit. Bjørn sier avslutningsvis i sitt intervju:

> «Sånn at jeg ser hvor verdifullt det er for Norge som land at befolkningen har stor tillit til politiet. Jeg ser at det er en kjemperessurs som igjen sparer en masse ressurser for samfunnet. Fordi det er mange ting vi ikke trenger å gjøre fordi vi stoler på politiet. Masse kontrollmekanismer som andre land må nødt å gjøre. Den tilliten må vi passe på. (...) jeg legger min ære i at når vi tar i bruk denne typen teknologi, så skal ikke det ende i en situasjon hvor det tærer på den tilliten».

Forskning som omhandler teknologiutvikling i politiet, viser til at det i dag finnes viktige etiske retningslinjer som politimyndigheter må forholde seg til. Disse har utgangspunkt i personvern, menneskerettigheter, rettferdighet og transparens (Klepper, et al., 2021, s. 41). Både informantene og forskning understøtter at transparens er helt nødvendig for å kunne skape tillitsfull bruk av forebyggende teknologi. Utgangspunktet er at vi ikke kan forstå teknologi uten å rette oppmerksomheten mot kunnskapsprosessene rundt teknologiene, samt innvirkningen de har på samfunnet (Flyverbom, 2019, s. 18).

6 Oppsummering

Jeg vil først oppsummere sentrale funn fra analysedelen av avhandlingen. Deretter vil jeg ha en mer overordnet diskusjon av øvrige funn ut fra teoretiske perspektiver og hvilke utviklingstrekk, utfordringer og viktige aspekter som kan identifiseres ut fra avhandlingen. Til slutt vil jeg kort redegjøre for mitt bidrag og komme med forslag til videre forskning på feltet.

6.1 Informantenes beskrivelser av en teknologisk utvikling

Som avdekket i avhandlingens første analysedel finner vi svært like definisjonsavklaringer på sentrale tekniske begreper. Både kunstig intelligens og maskinlæring blir i hovedtrekk beskrevet likt av informantene. Det generelle inntrykket er at kunstig intelligens er en form for overordnet maskinlæring, i tråd med pågående forskning på feltet. Samtidig beskriver informantene en flytende overgang mellom begrepene. Et annet likhetstrekk hos informantene, er deres fremtidsrettede syn på teknologi. Dette fremkommer i analysens andre del. Informantene veier både positive og negative sider ved utvikling og implementering av kriminalitetsforebyggende teknologibruk. Noen viser til en tydelig kompleksitet i teknologien. Andre tolker en del av kritikken mot forebyggende teknologi som uberettiget. Flertallet fremmer samtidig et balansert syn, som unngår å krisemaksimere teknologiens potensielle negative implikasjoner.

I analysens tredje del blir andre lands erfaringer diskutert. Også her er det samsvarende beskrivelser i de ulike intervjuene. Informantene er i første omgang opptatt av å tydeliggjøre hvor Norge ikke skal se. Kina og USA er landene der maktmisbruk, overdreven overvåkning og skjeve teknologier blir nevnt. Likevel blir det hevdet at det finnes noen interessante aspekter ved disse landenes teknologiutvikling som Norge kan lære av. Nederland er landet som informantene mener har kommet langt i en positiv utvikling innen forebyggende teknologi. Deres innovasjonsprosesser og etiske retningslinjer blir spesielt trukket frem. I tillegg beskriver flertallet EU som et fyrtårn innenfor lovverk på det teknologiske feltet. Det faktum at Norge er underlagt EUs regelverk, blir av informantene ansett som positivt, til tross for at dette resulterer i en saktegående teknologiinnovasjon for politimyndigheter. Det landet informantene er mest ambivalente til, er Storbritannia. Her blir bruken av overvåkningskamera og ansiktsgjenkjenning trukket frem som mest problematisk. Likevel fremkommer det at Storbritannia har «bevegelse i terrenget» som norske myndigheter bør ta etter. Felles for informantene er tydelige beskrivelser av det mulighetsrommet som forebyggende teknologi har.

6.2 (Mangelen på) motstand til teknologi i Norge

Avhandlingen har hatt utgangspunkt i en norsk kontekst, men har samtidig trukket linjer til andre land og aktører der dette har vært relevant. Funnene mine viser lite motstand til ulike forebyggende teknologier innad i Norge. Internasjonalt ser vi tydelig en annen tendens. Dette fremkommer både i avhandlingen og i øvrig forskningslitteratur. Aktivister og ulike grupper har stått i fronten for en debatt rundt de kritiske aspekter ved moderne teknologi (Chan, 2021, s. 48). En slik diskusjon blir spesielt viktig for bruken av kunstig intelligens i politiet. Grupper som fremmer menneskerettigheter stiller spørsmålstegn ved hvorvidt fordelene av at politimyndigheter benytter KI veier opp for de negative implikasjonene ved bruken (Chan, 2021, ss. 48-49). En sentral del av en slik kritikk er hvilken rolle teknologi skal ha for hvordan samfunnet organiseres og styres (Taylor, 2017, s. 10).

Flertallet av informantene mener at dagens forebyggende teknologi i Norge utvikles og implementeres i tråd med den eksisterende samfunnstilliten. Dette kan være noe av forklaringen på hvorfor det generelt har vært lite motstand mot slik teknologi i Norge. Den kritikken som har kommet, har kommet «innenfra» av fagpersoner, teknologer, myndighetspersoner, gravejournalister eller andre med inngående kjennskap til teknologi. Palantir-prosjektet er et godt eksempel på dette. Utover dette ser vi generelt få kritiske røster «utenfra» i den øvrige befolkningen.

Informantene i dette prosjektet er aktører på et felt som skal bringe frem teknologi i det norske samfunnet. De er svært opptatt av å gjøre det nøye og på en god måte. Jeg tolker informantene dithen at det er en tydelig bevissthet om at man må gå forsiktig frem. Informantene fremmer tydelige narrativ av at dette er en del av årsaken til at norske myndigheter ligger langt bak i teknologiutviklingen. En informant beskriver viktigheten av «å se til andre land og undersøke deres overførbarhet». En annen informant mener at en saktegående utvikling er viktig siden «det kan være vanskelig å putte ånden tilbake i flasken når den først er sluppet ut». Informantene viser til viktigheten av gjennomtenkte prosesser rundt teknologien. En slik tilnærming skal gjenspeile den tilliten norske myndigheter har i samfunnet i dag.

6.3 Overvåkning, forebygging og tillit – noen mulige implikasjoner og tendenser

Jeg vil nå sette funnene i analysen inn i en bredere sosial kontekst. Analysens funn vil samtidig knyttes opp mot avhandlingens teoretiske grunnlag.

6.3.1 Teknologiens overvåkningspotensial

I fjerde analysekapittel har jeg undersøkt hvilke utfordringer informantene mener forebyggende teknologi kan medføre. Mangelen på innsyn, personvern og ansvarsfordeling i teknologiutvikling fremheves som viktige problemstillinger. Underliggende skjevheter og bias i samfunnet som plukkes opp og integreres i data, er ifølge informantene også sentralt i en slik diskusjon. I tillegg beskriver de hvordan overdreven bruk av teknologi eller teknologi som brukes utenfor sin opprinnelige hensikt, vil være i strid med en tillitsfull forebyggende praksis. Samtidig blir overvåkningspotensialet som teknologi innehar ofte trukket frem i intervjuene.

Utgangspunktet for prosjektet har som nevnt innledningsvis vært det underliggende kritiske synet på teknologi som fremmes i forskningslitteraturen. Avhandlingen har vist til at politiets bruk av algoritmestyrte verktøy har blitt knyttet til ekskluderende praksiser i andre land. Det har samtidig blitt avdekket at forebyggende teknologi kan inneha omdiskuterte metoder som retter seg mot alle deler av befolkningen i et samfunn. Konsekvensen av dette er at forebyggende teknologi settes i sammenheng med diskurser av overvåkning. Som tidligere beskrevet viser Brayne (2022, s. 374) til hvordan digital teknologi stadig intensiverer overvåkningskapasiteten. Gjennom politiets bruk av prediktive verktøy som benytter KI og ML, blir overvåkningen mer omfattende enn før. I dag inngår også stordata i større grad enn tidligere i politiets overvåkning. Brayne (2017, s. 985) definerer dette som «stordataovervåkning». Utgangspunktet for en slik «stordataovervåkning» er at vi frivillig gir fra oss data i sosiale medier og på ulike plattformer. Disse dataene spores og lagres av private selskap som selger de videre (Zuboff, 2019). Denne prosessen har tidligere i avhandlingen blitt definert som «dataøkonomi». Slike datasamlinger kan også kjøpes opp av et lands myndigheter. På denne måten får myndigheter muligheten til å drive overvåkning og kontroll ved bruk av integrert stordata (Zuboff, 2019).Vi kan snakke om en type teknologi som er enda mer «finmasket», og som fanger opp enda flere enn tidligere. Dette inkluderer også samfunnsmedlemmer som ikke har begått lovbrudd.

Det er bred enighet i forskningslitteraturen om at det er en økende utbredelse av dagens overvåkning. Dette har resultert i at vi i dag henviser til fremveksten av «masseovervåkning» (Brayne, 2017, s. 978). En slik masseovervåkning kan tydelig settes i sammenheng med myndigheters bruk av stordata. Selv tror jeg at det er her kjernen i det underliggende kritiske synet ligger og at dette er en medvirkende faktor til at kriminalitetsforebygging ved bruk av teknologi tolkes som «farlig» eller «skremmende». Politiets bruk av ny teknologi blir ansett som en tydelig omfattende utvidelse av den overvåkende kontrollen. Eksempelvis har vi sett i intervjuene hvordan en negativ bruk av forebyggende teknologi i Kina og USA blir beskrevet i lys av deres masseovervåkningspraksiser. Den kritiske tolkningen handler nettopp om at hele befolkningen i et samfunn kan overvåkes i alle livssfærer. Kanskje er det derfor slik at vi kan snakke om en skepsis mot masseovervåkning, mer enn en skepsis mot forebyggende teknologi? Jeg mener det er viktig å skille mellom forebyggende teknologi som anses som nødvendig for å skulle drive forebyggende virksomhet i dag, og bruken av teknologi til masseovervåkning.

En tillitsfull bruk av forebyggende teknologi, vil ifølge informantene være mulig dersom samfunnet legger til rette for det. Inntrykket av en dyster teknologisk fremtid er altså ikke noe informantene fremmer: Tvert imot beskriver de hvordan teknologien vil kunne være et nyttig hjelpemiddel for norske myndigheter forutsatt at teknologien brukes riktig. Thomas Mathiesens (2013, s. 150) spådommer om en udemokratisk og autoritær fremtid, beskriver nettopp en statlig inngripende overvåkning som beveger seg mot det han omtaler som et «overvåkningssamfunn». Informantenes narrativ kan tolkes dithen at dette ikke nødvendigvis må være fremtiden til det norske samfunnet. Noen av informantene uttrykker at vi kanskje er unødvendig kritisk til teknologiutviklingen som foregår. Alle informantene fremmer en teknologioptimisme, men denne optimismen kommer med noen forutsetninger. De viser til risikoen av at frihet og trygghet kan risikere å komme i konflikt med hverandre, hvis ikke teknologiutviklingen drives frem forsiktig og på en god måte.

6.3.2 Det elastiske forebyggingsbegrepet

Et begrep som gjennomgående har blitt brukt i avhandlingen er «forebygging». Som vist til i kapittel 2, tolkes dette som elastisk i sin tilnærming (Gundhus, 2014, s. 179). Dette har i kapittel 3 blitt tydeliggjort gjennom Zedner og Ashworths (2014, s. 11) beskrivelser av skiftet i hvordan myndigheter tenker rundt forebygging. I dag handler forebygging mer om å forsøke å identifisere og nøytralisere potensielt farlige individer *før* de begår lovbrudd, fremfor å drive forebygging gjennom avskrekking og rehabilitering. En slik form for forebygging har beveget

seg videre inn i en foregripende praksis. Dette er i tråd med pre-kriminaliteten som avhandlingen har beskrevet. Pre-kriminaliteten ønsker å foregripe fremtiden, gjennom målrettet inngripen der det anses som nødvendig (McCulloch & Wilson, 2017, s. 48).

Det er interessant å se hvordan informantene tydelig fremmer en kriminalitetsforebygging med slike foregripende teknologier, fremfor en tradisjonell forståelse som handler om å analysere en situasjon, for så å sette inn tiltak mot situasjonen. I intervjuene er informantene i stor grad kortsiktige i forhold til prediksjon rundt forebygging. De har et tydelig ønske om presisjon og et behov for treffsikre og presise prediksjoner som skaper muligheter for at politiet kan drive foregripende praksis. Vi kan se dette i informantenes beskrivelser gjennomgående i analysen: i trianguleringsteknologi, i Entry/Exit-System for grensekontroll, i teknologi for ANRP-skiltgjenkjenning og i Nettprat-prosjektet. Vi kan eksempelvis trekke frem ANPR: Utgangspunktet for slik teknologi er å detektere i søkeregistre om personer har vært innblandet i lovbrudd. En slik prosess skal kunne skje fortløpende samtidig som politiet er ute i felten, noe som også vil resultere i en umiddelbar reaksjon av politiet. Vi kan derfor snakke om nærstående hendelser som skal forebygges.

Innsamlingen av sanntidsdata er samtidig et gjennomgående fellestrekk for teknologiene som beskrives av informantene. Teknologien har gjerne utgangspunkt i å søke i ulike databaser, for å kunne få frem analyser av individer eller gjenstander. En slik visualisering av databaser skal kunne gi politiet informasjon som de kan handle på umiddelbart eller i nær fremtid. Informantene viser samtidig til ønsket om data som kan skape muligheter for en praksis av presisjon, hvor de kan ha mulighet til å gripe inn raskt. Det er dermed teknologi som krever en «hands on»-tilnærming til forebygging. Alle disse teknologiene har utgangspunkt i prediksjonsteori i politiet. Fremtidige forestillinger om potensielle trusler legger grunnlaget for en slik tankegang (McCulloch & Wilson, 2017, s. 49). Det er nettopp dette som er pre-kriminalitetens virkeområde; hvor samfunnets sikkerhet er utgangspunktet for myndigheters praksis.

På ene siden kan en slik inngripende praksis være positivt for politiet. De vil naturligvis kunne ha et større handlingsrom for å arbeide preventivt, noe som igjen vil kunne forhindre fremtidig kriminalitet. På andre siden vil dette ha konsekvenser for politimyndigheter. Det er ikke bare forebyggingsbegrepet som blir mer elastisk, men også politirollen. Det at en inngripende praksis driver kriminalitetskontrollen, vil kunne forandre politiets virksomhet og mandat. Spørsmål

som kan stilles er derved hvordan en slik endring vil kunne påvirke politiet. Et annet spørsmål er hvor foregripende vi egentlig skal være før det vil komme i konflikt med de prinsipper det norske samfunnet står for. Følgende spørsmål er viktig å stille: vil en slik praksis av foregripende aktiviteter risikere å komme i konflikt med tillitsbegrepet? Som vi har sett i avhandlingen, vil dette i tilfelle kunne ha uheldige implikasjoner for den posisjonen som norske myndigheter innehar i Norge i dag.

6.3.3 Tillitens kompleksitet

I det femte og siste analysekapittelet beskriver informantene hvilke faktorer de mener er viktige for å tilrettelegge for en tillitsfull teknologiutvikling. Det er tydelig at informantene mener at dette vil være mulig dersom de rette forutsetningene legges til grunn. De mener for det første at det må legges til rette for kunnskap og kompetanse om teknologi i politiet. Dette blir fremhevet som viktig for å ivareta norske myndigheters legitimitet og tillit i samfunnet. Det blir også fremmet et narrativ av at noe av den kritikken som finnes mot forebyggende teknologi, bunner i kunnskapsmangel. Uttesting og kunnskapsdeling innad i politiet blir trukket frem som spesielt viktig. For det andre beskriver de at teknologien må inneha et godt datagrunnlag; teknologiske sandkassemiljøer, sammenkobling av relevante registre, åpenhet av underliggende og etablerte skjevheter, samt at det må stilles krav til presisjon i data. Det påpekes for det tredje at det må legges til rette for ansvarsfordeling og tverrfaglighet i politiet, samt hos øvrige instanser. Det vises til at dette kan være med på å øke kunnskapen rundt teknologi. Til slutt mener informantene at alle prosesser rundt forebyggende teknologi krever transparens. Dette vil ifølge informantene gjelde både i utviklingen av teknologi, i implementeringen av den, i etterprøvbarheten av den og i den praktiske bruken av den. Informantene er tydelige i sine tolkninger på at dette er en forutsetning for tillitsfull forebyggende teknologi. Åpenhet og redegjørelse for ulike teknologiske avveininger og etablerte skjevheter i samfunnet blir beskrevet som svært viktig i denne sammenhengen. Spørsmålet er om hvorvidt dette lar seg gjøre i praksis. Har for eksempel Norge ressursene til dette? Og vil det bli en utfordring at teknologiutviklingen i Norge drives frem sakte, når den i andre vestlige land går raskt?

Et siste spørsmål er hvor realistisk det er at norske myndigheter vil kunne drive foregripende forebygging ved bruk av teknologi på en tillitsfull måte. Informantene gir eksempelvis beskrivelser av at et godt datagrunnlag «skal gjenspeile den faktiske verden». Likevel har forskningslitteraturen vist oss at data alltid vil være utsnitt av *noens* virkelighet, og ikke den *faktiske virkeligheten*. Samtidig har avhandlingen avdekket at skjevheter uansett alltid vil prege

data. På tross av at ingen av informantene konkret snakker om «data justice», finnes det en bevissthet rundt dette. Det faktum at dataene vi henter inn i ulike datamodeller vil være skjeve i seg selv, er en viktig del av det som inngår i datarettferdighet. En antagelse er derfor at det i fremtiden vil være behov for en videre diskusjon om hva tillitsfull teknologi faktisk er. Det er tydelig at teknologien er et felt i konstant endring. En slik endring forsterkes av kunstig intelligens og maskinlæring i prediktive verktøy. Informantene uttrykker gjennomgående i intervjuene sine forestillinger av teknologiens muligheter og hva de tenker kan ha en overførbarhet til Norge.

Verdien av samfunnstillit er stor, og bør ifølge informantene på ingen måte rokkes ved. Dette er krevende i en verden som i økende grad setter trygghet og sikkerhet svært høyt. Vi risikerer at det som teknologi kan hjelpe oss med, også går på bekostning av de verdier og prinsipper som det norske samfunnet står for: «Teknologien kan bringe en mot et mål; for eksempel økt kapabilitet, men hvis den ikke har aksept i samfunnet kan teknologien også bidra til å skyve en bort fra det samfunnet en skal beskytte» (Klepper, et al., 2021, s. 43). En slik aksept forutsetter ifølge informantene at samfunnet har tillit til politiets metoder for forebygging.

Det siste kapittelet i avhandlingen fremmer håp og drømmer om fremtidens kriminalitetsforebygging. Informantenes tolkning er at forebyggende teknologi kan anses som noe som kan tilføre norske myndigheter noe positivt i deres forebyggende praksis. Jeg introduserte i innledningen av avhandlingen et sitat om puslespillbrikker. Jeg vil avslutningsvis konkludere med en oversettelse av den analogien: «For at forebyggende teknologi skal bidra i positiv forstand må teknologien bli brukt med forsiktighet. Hvis ny forebyggende teknologi blir implementert og brukes overdrevent (eksempelvis i form av å erstatte mennesker), blir ansett som viktigere enn den faktisk er eller i verste fall brukes på en måte som ikke var tiltenkt i utgangspunktet; er det godt mulig at den gjør mer skade enn nytte». Dette sitatet mener jeg oppsummerer informantenes syn på tillitsfull teknologi.

6.4 Avslutning

I avhandlingens avslutning ønsker jeg å trekke frem igjen studiens problemstilling: «*Hvordan kan vi skape en tillitsfull bruk av forebyggende teknologi for å forebygge fremtidig kriminalitet?*». For å besvare dette har jeg i første omgang belyst hvilke forestillinger fagpersoner har om fremtidens forebygging. Informantene viser til en forsiktig teknologioptimisme, som forutsetter at de riktige forutsetningene ligger til rette. Jeg har så trukket linjer til de landene og aktørene som informantene mener Norge bør la seg inspirere av når det kommer til en slik teknologiimplementering. Nederland og EU er tydelig der informantene mener det foregår en positiv teknologiutvikling og implementering. Informantene har noe varierte tilnærminger til Storbritannia. USA og Kina trekkes frem som eksempler på land det norske samfunnet ikke bør la seg inspirere av. Videre har jeg sett nærmere på de ulike utfordringer som finnes ved en forebyggende teknologibruk. Her har mangelen på innsyn, personvern, etiske problemstillinger, skjevheter, bias og utfordringer rundt tillit vært hovedtrekkene som informantene beskriver. Jeg har deretter belyst informantenes tolkninger av hvordan det norske samfunnet kan tilrettelegge for en praksis av tillitsfull kriminalitetsforebygging ved bruk av teknologi. Informantene viser til at kunnskap og kompetanse, tverrfaglighet og ansvarsfordeling, godt datagrunnlag og transparens ligger til grunn. Prosjektets tematikk er gjennomgående diskutert i lys av kriminologisk teori og relevant tidligere forskning.

Sentrale funn som kan trekkes frem er at informantene i stor grad er enige med hverandre tross sine ulike faglige utgangspunkt, samt at informantene fremmer en foregripende forebyggingspraksis. Ut ifra informantenes synspunkt, er det tydelig en villighet og et ønske om å skape gode rammer rundt fremtidens forebygging. Samtidig er det viktig å stille spørsmålstegn ved om politiet er forberedt på å gå en slik utvikling i møte. Prosjektets informanter er fagpersoner på det aktuelle feltet. De er valgt ut nettopp fordi de påvirker landskapet av forebyggende teknologi. Informantene er derfor godt egnet til å besvare problemstillingen, og det er viktig å ta innover seg de mangler, implikasjoner og utfordringer som informantene mener finnes i dag. Det er samtidig viktig å se nærmere på deres tolkninger av hva som kreves for en tillitsfull bruk av forebyggende teknologi.

Foruten å besvare avhandlingens problemstilling, har denne studien forhåpentligvis bidratt noe med å øke bevisstheten rundt problematikk knyttet til forebyggende teknologiutvikling i polisiær virksomhet. Som nevnt i de foregående kapitler er teknologi som innebefatter kunstig

intelligens og maskinlæring lite tematisert i det fremvoksende feltet digital kriminologi. Avhandlingen har forhåpentligvis tydeliggjort behovet for mer kunnskap rundt dette innenfor kriminologien. Hensikten har samtidig vært å undersøke hvordan vi kan sikre en åpen demokratisk debatt om politiets bruk av prediktiv analyse, som i utgangspunktet er et spesialisert kompetanseområde. Når det gjelder videre forskning hadde det vært interessant å gjøre en lignende studie når teknologiutviklingen har kommet lengre enn den har i dag. Her kunne man sett om hvorvidt den teknologiske utviklingen har vært i tråd med informantenes tolkninger av det som inngår i tillitsfull kriminalitetsforebygging. Denne avhandlingen ønsker å være med på å belyse den utviklingen det norske samfunnet går i møte på dette feltet.

Antall ord: 41452

7 Litteraturliste

Almås, G. B. (2019, 5. februar). *Digitalt diktatur: Kina planlegger sosialt poengsystem*. Hentet fra NRK: https://www.nrk.no/urix/kinas-digitale-diktatur_-gar-du-pa-rodt-lys_-blir-du-uthengt-pa-storskjerm-1.14369439

Amnesty International. (2020, 25. februar). *Ikke trygg noe sted*. Hentet fra https://amnesty.no/aksjon/ikke-trygg-noe-sted

Aas, K. F. (2013). *Globalization and crime.* (2. utgave) London: Sage.

Aas, K. F. (2014). Bordered penality: Precarious membership and abnormal justice. *Punishment & Society, 16(5)*, ss. 520-541. https://doi.org/10.1177/1462474514548807.

Aas, K. F., Gundhus, H. O., & Lomell, H. M. (Red.). (2009). *Technology of Insecurity.* Oxon og New York: Routledge-Cavendish.

Barkane, I. (2022). Questioning the EU proposal for an Artificial Intelligence Act: The need for prohibitions and a stricter approach to biometric surveillance. *Information Polity, 27(2)*, ss. 147-162. https://doi.org/10.3233/IP-211524.

Brayne, S. (2017). Big data surveillance: The case of policing. *American Sociological Review, 82(5)*, ss. 977-1008. https://doi.org/10.1177/000312241772586.

Brayne, S. (2022). The Banality of Surveillance. *Surveillance and Society, 20(4)*, ss. 372-378. https://doi.org/10.24908/ss.v20i4.15946.

Brekke, A., & Helljesen, V. (2020, 29. april). *Hagen-forsvinningen: Dette er politiets spor så langt*. Hentet fra NRK: https://www.nrk.no/norge/anne-elisabeth-hagen-forsvinningen_-dette-er-politiets-spor-sa-langt-1.14998946

Brinkmann, S., & Kvale, S. (2018). *Doing Interviews.* (2. utgave) London: Sage Publications Ltd.

Bukve, O. (2021). *Forstå forklare forandre: Om design av samfunnsvitenskapelige forskningsprosjekt.* Oslo: Universitetsforlaget.

Byrne, J., & Marx, G. (2011). Technological Innovations in Crime Prevention and Policing. A Review of the Research on Implementation and Impact. *Journal of Police Studies, 3(20)*, ss. 17-40.

Chan, J. (2021). The future of AI in policing: Exploring the sociotechnical imaginaries. I J. McDaniel, & K. Pease, *Predictive Policing and Artificial Intelligence* (ss. 41-58). London: Routledge.

Chan, J., & Moses, L. B. (2018). Algorithmic prediction in policing: assumptions, evaluation, and accountability. *Policing and Society, 28(7)*, ss. 806-822. https://doi.org/10.1080/10439463.2016.1253695.

Chriss, J. (2012). *Social Control: An Introduction.* (2. utgave) Cambridge og Malden: Polity Press.

Clarke, R. V. (1995). Situational Crime Prevention. *Crime and Justice, 19*, ss. 91-150.

Cohen, S. (1979). The punitive city: Notes on the dispersal of social control. *Contemporary Crises, 3*, ss. 339-363. https://doi.org/10.1007/BF00729115.

Council of the European Union. (2020, 21. oktober). *Artificial intelligence: Presidency issues conclusions on ensuring respect for fundamental rights.* Hentet fra https://www.consilium.europa.eu/en/press/press-releases/2020/10/21/artificial-intelligence-presidency-issues-conclusions-on-ensuring-respect-for-fundamental-rights/

Datatilsynet. (2019, 8. august). *Ha behandlingsgrunnlag*. Hentet fra https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/behandlingsgrunnlag/veileder-om-behandlingsgrunnlag/

Datatilsynet. (2020, 26. mai). *Starter regulatorisk sandkasse for utvikling av ansvarlig kunstig intelligens*. Hentet fra https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/regulatorisk-sandkasse-for-utvikling-av-ansvarlig-kunstig-intelligens/

Döringer, S. (2021). 'The problem-centred expert interview'. Combining qualitative interviewing approaches for investigating implicit expert knowledge. *International Journal of Social Research Methodology, 24(3)*, ss. 265-278. https://doi.org/10.1080/13645579.2020.1766777.

Dencik, L., & Sanchez-Monedero, J. (2022). Data justice. *Internet Policy Review: Journal of internet regulation, 11(1)*, ss. 1-16. https://doi.org/10.14763/2022.1.1615 .

Ditlefsen, H., Arntzen, K. J., & Egeland, G. I. (2018, 5. mars). *Her jaktes overgripere - nå kommer politiet på døra*. Hentet fra NRK: https://www.nrk.no/sorlandet/operasjon-dark-room-i-agder-fylkene-1.13936917

Dodd, V. (2022, 27. oktober). *UK police use of live facial recognition unlawful and unethical, report finds*. Hentet fra The Guardian: https://www.theguardian.com/technology/2022/oct/27/live-facial-recognition-police-study-uk

Earle, R., Parmar, A., Phillips, C., & Smith, D. (2020). Dear British criminology: Where has all the race and racism gone? *Theoretical Criminology, 24(3),* ss. 427-446. https://doi.org/10.1177/1362480619880345.

Egge, M., Strype, J., & Thomassen, G. (2012). *Tillit til politiet etter 22. juli.* (PHS forskning 2012:5) Oslo: Politihøgskolen.

Ericson, R. V., & Haggerty, K. D. (2000). The surveillant assemblage. *The British Journal of Sociology, 51(4),* ss. 605-622. https://doi.org/10.1080/00071310020015280.

Eriksen, D. (2022, 7. desember). *Lærere fortvilet over ny kunstig intelligens*. Hentet fra NRK: https://www.nrk.no/kultur/laerere-fortvilet-over-ny-kunstig-intelligens-1.16210580

EU. (u.å.). *New requirements to travel to Europe*. Hentet fra https://travel-europe.europa.eu/ees/general-information_en

European Commision. (2023, 26. januar). *A European approach to artificial intelligence*. Hentet fra https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence

Europol. (2022, 17. oktober). *Innovation lab*. Hentet fra https://www.europol.europa.eu/operations-services-and-innovation/innovation-lab

Feeley, M., & Simon, J. (1992). The New Penology: Notes on the Emerging Strategy of Corrections and Its Implications. *Criminology, 30(4)*, ss. 449-474. https://doi.org/10.1111/j.1745-9125.1992.tb01112.x.

Fekjær, S. B. (2022). *Hvordan bli en lykkelig masterstudent: Masteroppgavehåndbok.* Oslo: Gyldendal.

Flyverbom, M. (2019). *Digital Prism: Transparency and Managed Visibilities in a Datafied World.* Cambridge: Cambridge University Press.

Flyverbom, M., & Koed Madsen, A. (2015). Sorting Data Out: Unpacking Big Data Value Chains and Algoritmic Knowlegde Production. I *Die Gesellschaft der Daten* (ss. 123-144. https://doi.org/10.1515/9783839427644-006). Transcript Verlag.

Flyverbom, M., & Murray, J. (2018). Datastructuring—Organizing and curating digital traces into action. *Big Data and Society, 5(2)*, ss. 1-12. https://doi.org/10.1177/2053951718799114.

Furseth, I., & Everett, E. L. (2020). *Masteroppgaven: Hvordan begynne - og fullføre.* (3. utgave) Oslo: Universitetsforlaget.

Future of life Institute. (2023, 22. mars). *Pause Giant AI Experiments: An Open Letter*. Hentet fra https://futureoflife.org/open-letter/pause-giant-ai-experiments/

Fyfe, N. R., Gundhus, H. O., & Rønn, K. V. (Red.). (2018). *Moral Issues In Intelligence-led Policing.* London og New York: Routledge Raylot and Francis Group.

Goodwin, M. (2020). *AI: Myten om maskiene.* Oslo: Humanist forlag AS.

Grut, S. (2021, 17. desember). *«Supervåpen» fra Silicon Valley ga hodebry og millionsprekk for politiet*. Hentet fra NRK beta: https://nrkbeta.no/2021/12/17/supervapen-fra-silicon-valley-ga-hodebry-og-millionsprekk-for-politiet/

Gundhus, H. O. (2014). Forebyggende politiarbeid – i spennet mellom kriminalitetskontroll og trygghet. I P. Larsson, H. O. Gundhus, & R. Graner (Red.), *Innføring i politivitenskap* (ss. 178-204). Oslo: Cappelen Damm akademisk.

Hansen, Ø. S. (2019, 6. desember). *Dette landet har flest overvåkningskameraer* . Hentet fra Itavisen: https://itavisen.no/2019/12/06/dette-landet-har-flest-overvakningskameraer/

Hennink, M., Hutter, I., & Bailey, A. (2020). *Qualitative Research Methods* (Vol. 2. utgave). (2. utgave) London: Sage Publications Ltd.

Holm-Nilsen, S., & Sølhusvik, L. (2023, 27. januar). *Norsk politi bidro til å stanse hackergigant*. Hentet fra NRK: https://www.nrk.no/norge/dataangriperne-bak-amedia-hackingen-stanset-av-fbi-1.16273214

Hunt, G., Wästerfors, D., Kolind, T., Saarikkomäki, E., Solhjell, R., & Haller, M. B. (2020). Minor harassments: Ethnic minority youth in the Nordic countries and their perceptions of the police. *Criminology & Criminal Justice, 20(1)*, ss. 3-20. https://doi.org/10.1177/1748895818800744.

Iliadis, A., & Acker, A. (2022). The seer and the seen: Surveying Palantir's surveillance platform. *The Information Society, 38(5)*, ss. 334-363. https://doi.org/10.1080/01972243.2022.2100851.

Inderhaug, E. (2014, 17. september). *Dette kameraet gjør politiet fem ganger så effektive*. Hentet fra Politiforum: https://www.politiforum.no/nyheter/dette-kameraet-gjor-politiet-fem-ganger-sa-effektive/118757

Inderhaug, E. (2016, 29. september). *Nå dobler politiet ANPR-kapasiteten*. Hentet fra Politiforum: https://www.politiforum.no/nyheter/na-dobler-politiet-anpr-kapasiteten/132456

Iversen, M. (2019, 31. mars). *Teknologi gjør millioner til annenrangs innbyggere*. Hentet fra DN: https://www.dn.no/utenriks/kina/sosial-kreditt/teknologi-gjor-millioner-til-annenrangs-innbyggere/2-1-576853

Jørgensund, M. (2017, 14. februar). *Hemmelighetsfulle Palantir starter opp i Norge*. Hentet fra Digi: https://www.digi.no/artikler/hemmelighetsfulle-palantir-starter-opp-i-norge/376585

Johannessen, S. Ø. (2019, 11. januar). *Ekspert om kryptokrav: Skjer i gjennomsnitt én gang i måneden globalt* . Hentet fra DN: https://www.dn.no/marked/nicola-white/control-risks/anne-elisabeth-falkevik-hagen/ekspert-om-kryptokrav-skjer-i-gjennomsnitt-en-gang-i-maneden-globalt/2-1-517370

Justis- og beredskapsdepartementet. (2022). Prop. 31 L (2022–2023). *Endringer i politiloven og politiregisterloven (PSTs etterretningsoppdrag og bruk av åpent tilgjengelig informasjon)*. https://www.regjeringen.no/no/dokumenter/prop.-31-l-20222023/id2949174/?ch=1: Justis- og beredskapsdepartementet.

Kaufman, M. (2018). Kriminalitetskontroll eller sikkerhetspolitikk? *Nytt norsk tidsskrift, 35(1)*, ss. 21-31. https://doi.org/10.18261/issn.1504-3053-2018-01-03.

Kaufman, M., Egbert, S., & Leese, M. (2018). Predictive Policing and the Politics of Patterns. *The British Journal of Criminology, 59(3)*, ss. 674-692. https://doi.org/10.1093/bjc/azy060.

Kjelsberg, R. (2022). *Teknologi og vitenskap: Historie, metode, etikk og miljø.* (2. utgave) Oslo: Universitetsforlaget.

Klepper, K., Greve, B., Ousdal, S., Paulsen, J. E., Rjaanes, M., Strand, M., & Thorsberg, L. (2021). *Teknologiutviklingens betydning for politiet, PST og Den høyere påtalemyndighet.* (FFI-rapport 02532) Forsvarets forskningsinstitutt.

Knudsen, E. (2023, 11. februar). *Advarer: ChatGPT brukes allerede til å lage skadevare*. Hentet fra Digi: https://www.digi.no/artikler/advarer-chatgpt-brukes-allerede-til-a-lage-skadevare/526137

Kommunal- og moderniseringsdepartementet. (2020). *Nasjonal strategi for kunstig intelligens.*

Larsson, P., Eriksen, T., Pedersen, C., & Alvin, A. (2022). *Langsiktige trender i kriminalitetsbildet: Vurderinger av metoder for beskrivelse av fremtidig kriminalitetsutvikling.* (PHS forskning 2022: 8). Oslo Politihøgskolen.

Leese, M. (2014). The new profiling: Algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union. *Security dialogue: Special issue on Preemption, Practice, Politics, 45(5)*, ss. 494-511. https://doi.org/10.1177/0967010614544204.

Liebling, A., Maruna, S., & McAra, L. (Red.). (2019). *The Oxford handbook of criminology.* (sjette utgave). Oxford: Oxford University Press.

Lomell, H. M. (2012). Punishing the uncommitted crime: Prevention, pre-emption, precaution and the tranformation of criminal law. I B. Hudson, & S. Ugelvik, *Justice and Security in the 21st Century: Risks, rights and the rule of law* (ss. 83-100). London: Routledge.

Lyon, D. (2001). *Surveillance society: Monitoring Everyday Life.* Philadelphia: Open University Press.

Lyon, D. (Red.). (2003). *Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination.* New york: Routledge Taylor and Francis Group.

Lyon, D. (2007). *Surveillance Studies: An Overview.* Cambrigde: Polity Press.

Mathiesen, T. (2013). *Towards a survellant society: The rise of Surveillance systems in Europe.* UK: Waterside Press.

McCulloch, J., & Wilson, D. (2017). *Pre-crime: Pre-emption, precaution and the future.* London og New York: Routledge.

Mergel, I., Edelmann, N., & Haug, N. (2019). Defining digital transformation: Results from expert interviews. *Government Information Quarterly, 36(4)*, ss. 1-16. https://doi.org/10.1016/j.giq.2019.06.002.

Niculescu-Dincă, V. (2021). Theorizing Technologically Mediated Policing in Smart Cities: An Ethnographic Approach to Sensing Infrastructures in Security Practices. I M. Nagenborg, T. Stone, M. González Woge, & P. E. Vermass, *Technology and the City: Towards a Philosophy of Urban Technologies* (ss. 75-100). New York: Springer.

NL Times. (2021, 2. oktober). *License plate recognition cameras are "massive privacy violation": Privacy First*. Hentet fra https://nltimes.nl/2021/10/02/license-plate-recognition-cameras-massive-privacy-violation-privacy-first

Norli, C. (2023, 4. mai). *VG*. Hentet fra AI-bok utsolgt: Selger aller mest i Norge nå: https://www.vg.no/rampelys/bok/i/2BXMWa/ai-bok-utsolgt-inga-strumke-selger-aller-mest-i-norge-av-maskiner-som-tenker

Otterlei, S. S., & Øystese, O. (2017, 30. mai). *Nye Dark Room-tall: Minst 300 barn grovt seksuelt utnyttet og misbrukt*. Hentet fra NRK: https://www.nrk.no/vestland/nye-dark-room-tall_-minst-300-barn-grovt-seksuelt-utnyttet-og-misbrukt-1.13536946

Politidirektoratet. (2020). *I forkant av kriminaliteten.* Oslo: Politiet.

Politiet. (u. å.). *Organisasjonen*. Hentet fra https://www.politiet.no/om-politiet/organisasjonen/sarorganene/pit/om-pit/organisasjonen/

Politiloven. (1995). *Lov om politiet.* (LOV-1995-08-04-53): Lovdata: https://lovdata.no/LTI/lov/1995-08-04-53/§1.

Powell, A., Stratton, G., & Cameron, R. (2018). *Digital criminology: Crime and Justice in Digital Society.* New York og London: Routledge.

PST. (2023). *Nasjonal trusselvurdering 2023.* Politiets sikkerhetstjeneste.

Radiya-Dixit, E. (2022). *A Sociotechnical Audit: Assesing police use of facial recognition.* Cambrige: Minderloo Centre for Technology and Democracy.

Røyse, M. B. (2020, 5. mai). *Prestisjeprosjekt avsluttet etter 11 år: – Ser ut som 100 millioner er brukt uten å gi resultater*. Hentet fra DIgi: https://www.digi.no/artikler/prestisjeprosjekt-avsluttet-etter-11-ar-ser-ut-som-100-millioner-er-brukt-uten-a-gi-resultater/491448

Schengenvisa. (u.å.). *Entry/Exit System (EES)*. Hentet fra https://www.schengenvisainfo.com/entry-exit-system-ees/

Skilbrei, M.-L. (2021). *Kvalitative metoder: Planlegging, gjennomføring og etisk refleksjon.* Bergen: Fagbokforlaget.

Skilbrei, M.-L., & Haugen, H. Ø. (2021). *Håndbok i forskningsetikk og databehandling.* Bergen: Fagbokforlaget.

Skille, Ø. B. (2020, 9. mars). *Kripos søkte med bilder fra norske etterforskninger i omstridt app*. Hentet fra NRK: https://www.nrk.no/norge/kripos-sokte-med-bilder-fra-norske-etterforskninger-i-omstridt-app-1.14935430

Solheim, U., & Mematpoor, S. (2023, 23. april). *Etterlyser plan for kunstig intelligens: – Mens KI-toget går, står vi igjen på perrongen*. Hentet fra NRK: https://www.nrk.no/norge/etterlyser-plan-for-kunstig-intelligens_--_-mens-ki-toget-gar_-star-vi-igjen-pa-perrongen-1.16380120

Stanley, J. (2011, 11. desember). *Beware of Data Miners Offering Protection*. Hentet fra ACLU: https://www.aclu.org/news/privacy-technology/beware-data-miners-offering-protection

Sunde, I. M., Bendiksen, J., & Sunde, N. (2022). *Nettprat- prosjektet Bruk av nettprat-bevis innhentet i etterforsking som treningsdata til en lærende KI-modell.* (PHS forskning 2022: 5). Oslo: Politihøgskolen.

Sunde, N. (2022). Unpacking the evidenceelasticity of digital traces. *Cogent Social Sciences, 8(1),* ss. 1-18. https://doi.org/10.1080/23311886.2022.2103946.

Taylor, L. (2017). What is data justice? The case for connecting digital rights and freedoms globally. *Big Data & Society, 4(2)*, ss. 1-14. https://doi.org/10.1177/2053951717736335.

Teknologirådet. (2018). *Teknologirådets årsrapport for 2018*. Hentet fra Teknologirådet: Teknologiradets-arsrapport-for-2018.pdf (wpd.digital)

The United States Department of Justice. (2023, 26. januar). *U.S. Department of Justice Disrupts Hive Ransomware Variant*. Hentet fra Department of Justice Office of Public Affairs: https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant

Trædal, T. J. (2016, 10. mai). *ANPR-framtiden nederlandsk politi drømmer om*. Hentet fra Politiforum: https://www.politiforum.no/nyheter/anpr-framtiden-nederlandsk-politi-drommer-om/130027

Vestby, A. (2018). Policy making without politics: Overstating objectivity in intelligence led policing. I N. R. Fyfe, H. O. Gundhus, & K. V. Rønn (Red.), *Moral issues in intelligence-led policing* (ss. 265-280). UK: Routledge.

Vestby, A., & Vestby, J. (2019). Machine Learning and the Police: Asking the Right Questions. *Policing: A Journal of Policy and Practice, 15(1)*, ss. 44-58. https://doi.org/10.1093/police/paz035.

Wilson, D. (2019). Platform Policing and the Real-Time Cop. *Surveillance & Society, 17*, ss. 69-75. https://doi.org/10.24908/ss.v17i1/2.12958.

Østli Jakobsen, H. (2021). *Palantir i politiet.* Hentet fra SKUP Microsoft Word - Palantir Metoderapport.docx (skup.no).

Zedner, L. (2007). Pre-crime and post-criminology. *Theoretical Criminology, 11(2)*, ss. 261-281. https://doi.org/10.1177/1362480607075851.

Zedner, L. (2009). *Security.* UK: Routledge.

Zedner, L., & Ashworth, A. (2014). *Preventive Justice.* University of Oxford: Oxford University Press.

Zuboff, S. (2019). *The Age of Surveillance Capitalism.* London: Profile Books Ltd.

VEDLEGG 1: Godkjenning fra NSD

Vurdering av behandling av personopplysninger

Skriv ut | 26.08.2022

Referansenummer
302430

Vurderingstype
Standard

Dato
26.08.2022

Prosjekttittel
Bruken av kunstig intelligens i norsk kriminalitetsforebygging

Behandlingsansvarlig institusjon
Universitetet i Oslo / Det juridiske fakultet / Institutt for kriminologi og rettssosiologi

Prosjektansvarlig
[redacted]

Student
[redacted]

Prosjektperiode
16.05.2022 - 30.06.2023

Kategorier personopplysninger
Alminnelige

Lovlig grunnlag
Samtykke (Personvernforordningen art. 6 nr. 1 bokstav a)

Behandlingen av personopplysningene er lovlig så fremt den gjennomføres som oppgitt i meldeskjemaet. Det lovlige grunnlaget gjelder til 30.06.2023.

Meldeskjema

Kommentar
Personverntjenester har vurdert endringen registrert i meldeskjemaet.

Det er vår vurdering at behandlingen av personopplysninger i prosjektet vil være i samsvar med personvernlovgivningen så fremt den gjennomføres i tråd med det som er dokumentert i meldeskjemaet med vedlegg. Behandlingen kan fortsette.

ENDRING
Det er lagt til et nytt utvalg.

LOVLIG GRUNNLAG
Prosjektet vil innhente samtykke fra de registrerte til behandlingen av personopplysninger. Vår vurdering er at prosjektet legger opp til et samtykke i samsvar med kravene i art. 4 og 7, ved at det er en frivillig, spesifikk, informert og utvetydig bekreftelse som kan dokumenteres, og som den registrerte kan trekke tilbake.

Lovlig grunnlag for behandlingen vil dermed være den registrertes samtykke, jf. personvernforordningen art. 6 nr. 1 bokstav a.

DE REGISTRERTES RETTIGHETER
Så lenge de registrerte kan identifiseres i datamaterialet vil de ha følgende rettigheter: innsyn (art. 15), retting (art. 16), sletting (art. 17), begrensning (art. 18), og dataportabilitet (art. 20).

Personverntjenester vurderer at informasjonen om behandlingen som de registrerte vil motta oppfyller lovens krav til form og innhold, jf. art. 12.1 og art. 13.

Vi minner om at hvis en registrert tar kontakt om sine rettigheter, har behandlingsansvarlig institusjon plikt til å svare innen en måned.

OPPFØLGING AV PROSJEKTET
Vi vil følge opp ved planlagt avslutning for å avklare om behandlingen av personopplysningene er avsluttet.

Kontaktperson: Line Raknes Hjellvik
Lykke til videre med prosjektet!

VEDLEGG 2: Informasjonsskriv og samtykkeerklæring til informanter

Vil du delta i forskningsprosjektet

«Hvordan skape tillitsfulle algoritmer for politiet?»

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å undersøke hvordan kunstig intelligente algoritmer for kriminalitetsforebygging i Norge skal se ut. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål
Jeg ønsker å gå i dybden av hvordan en forsøker å få til utviklingen av algoritmer som en del av kriminalitetsforebyggingen og hvordan en slik etisk bruk av algoritmer skal kunne fungere i praksis i Norge. Mye tyder på dette i hovedsak foregår på utviklingsnivå fremfor i praksis hos norsk politi i dag. Det er også vanskelig å få tak på hvilke metoder som faktisk er tiltenkt å bruke og hvordan disse vil kunne virke. Jeg er derfor interessert i å undersøke hvordan bruken av KI hos norsk politivirksomhet skal se ut. Spørsmålene vil derfor dreie seg om hvordan kunstige intelligente systemer utvikles, på hvilket grunnlag de skapes og hvordan de vil se ut. Det er også sentralt å se på hvilken type kriminalitet slike KI-systemer skal forebygge. Prosjektet har følgende problemstilling: *Hvordan kan en skape en inkluderende praksis av kunstig intelligens i Norge?*

Studien som skal gjøres er i forbindelse med masterstudier ved Universitetet i Oslo.

Hvem er ansvarlig for forskningsprosjektet?
Juridisk fakultet/Institutt for kriminologi og rettssosiologi ved Universitetet i Oslo er ansvarlig for prosjektet.

Hvorfor får du spørsmål om å delta?
Utvalget er trukket på bakgrunn av at jeg ønsker å komme i kontakt med personer som utvikler kunstig intelligente systemer som skal brukes av politiet for å forebygge kriminalitet. Dette er i dag en liten gruppe som gjør i Norge. Dette gjør at mitt utvalg på tross av et lite antall informanter, kan være representativt for populasjonen.

Hva innebærer det for deg å delta?
Metode for innsamling av data er i denne studien kvalitative intervjuer. Hvis du velger å delta i prosjektet innebærer det derfor at du deltar i et intervju basert på en forhåndsskrevet intervjuguide. Intervjuet vil være en-til-en, og vil ta omtrent 45-60 minutter. Jeg vil ta notater underveis i intervjuene. Intervjuene vil også bli tatt opp med lydopptaker lånt fra Universitetet i Oslo. Bakgrunnen for at intervjuene blir tatt opp er for å sikre at intervjuet blir korrekt og ikke kan tas ut av kontekst. Disse lydopptakene vil bli transkribert, anonymisert og oppbevart elektronisk.

Om det skulle være ønskelig kan du på forhånd ta kontakt for øvrige eventuelle spørsmål.

Det er frivillig å delta
Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykket tilbake uten å oppgi noen grunn. Alle dine personopplysninger vil da bli slettet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger
Jeg vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Jeg vil behandle opplysningene konfidensielt og i samsvar med personvernregelverket. Det er jeg alene som gjennomfører masterprosjektet, og som vil ha tilgang til dine opplysninger og datamaterialet. Navnet og kontaktopplysningene dine vil erstattes med en kode som lagres på egen navneliste adskilt fra øvrige data. Datamaterialet vil lagres og oppbevares på UiOs brukersystem bak lukket tilgang ved hjelp av innloggingsfunksjon. Deltakerne i studien vil ikke spesifikt kunne gjenkjennes i publikasjonen gjennom informasjonen som publiseres.

Hva skjer med personopplysningene dine når forskningsprosjektet avsluttes?
Prosjektet vil etter planen avsluttes våren 2023, herunder mai måned. Etter prosjektslutt vil datamaterialet med dine personopplysninger slettes. De anonymiserte personopplysningene vil ikke gjenbrukes for videre forskning etter prosjektslutt.

Hva gir oss rett til å behandle personopplysninger om deg?
Jeg behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra Juridisk fakultet/Institutt for kriminologi og rettssosiologi ved Universitetet i Oslo har Personverntjenester vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Dine rettigheter
Så lenge du kan identifiseres i datamaterialet, har du rett til:

- Innsyn i hvilke opplysninger vi behandler om deg, og å få utlevert en kopi av opplysningene
- Å få rettet opplysninger om deg som er feil eller misvisende
- Å få slettet personopplysninger om deg
- Å sende klage til Datatilsynet om behandlingen av dine personopplysninger

Hvis du har spørsmål til studien, eller ønsker å vite mer om eller benytte deg av dine rettigheter, ta kontakt med:

[redacted]

Hvis du har spørsmål knyttet til Personverntjenester sin vurdering av prosjektet, kan du ta kontakt med:

- Personverntjenester på e-post (personverntjenester@sikt.no) eller på telefon: 53 21 15 00.

Med vennlig hilsen

[redacted]

VEDLEGG 3: Samtykkeerklæring fra informanter

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet *«Hvordan skape tillitsfulle algoritmer for politiet?»,* og har fått anledning til å stille spørsmål. Jeg samtykker til:

- ☐ Å delta i intervju
- ☐ At intervjuet blir tatt opp med lydopptaker
- ☐ At mine opplysninger behandles frem til prosjektet er avsluttet

---

(Signert av prosjektdeltaker, dato)

VEDLEGG 4: Intervjuguide

Intervjuguide:

- Kan du fortelle noe om hva du jobber med? Og litt om din arbeidserfaring?
- Hvordan definerer du kunstig intelligens?
- Kan du si noe om hva forskjellen på kunstig intelligens og maskinlæring er?
- Kan du forklare hvordan du jobber med utvikling av KI og hvordan denne typen teknologi fungerer?
- Hvilken type lovbrudd skal denne typen teknologier du arbeider med være med på å forebygge?
- Hvordan tenker du at bruken av teknologi og KI innenfor kriminalitetsforebygging skal kunne implementeres i politiet? (I hvor stor grad)
- Hvilke land ser mener du at vi skal se til når det kommer til implementeringen av teknologi og KI på samfunnsnivå og innenfor kriminalitetsforebygging?
- Hvilke typer lovbrudd mener du at KI skal være med på å forebygge? Og er det noen typer lovbrudd du spesifikt tenker at KI ikke skal inkludere?
- Hvilke holdninger har du til bruken av kunstig intelligens?
- Ser du spesielle etiske utfordringer ved bruken av KI innen kriminalitetsforebygging? I så fall hvilke?
- Tror du det er mulig å skape en tillitsfull bruk av KI?
- Har du avslutningsvis noe annet å legge til i forbindelse med spørsmålene jeg har stilt som du tenker at det er viktig å poengtere?